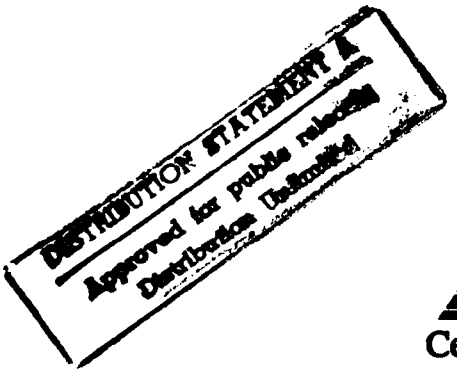
CDRL: B004
28 February 1994

UNISYS

Library Operations Policies and Procedures, Volume II

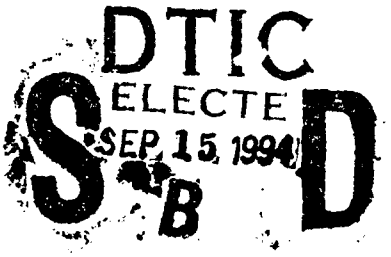
Central Archive for Reusable Defense Software (CARDS)

Informal Technical Report



Central Archive for Reusable Defense Software

STARS-VC-B004/002/01
28 February1994



INFORMAL TECHNICAL REPORT
For The
SOFTWARE TECHNOLOGY FOR ADAPTABLE, RELIABLE SYSTEMS
(STARS)

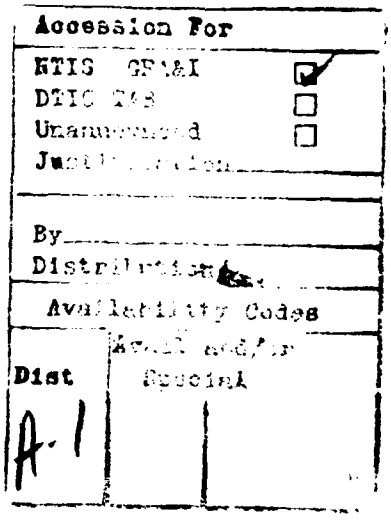
Library Operations Policies and Procedures, Volume II
Central Archive for Reusable Defense Software
(CARDS)

STARS-VC-B004/002/01
28 February 1994

Data Type: Informal Technical Data
Contract NO. F19628-93-C-0130
Line Item 0002AB

Prepared for:

Electronic Systems Center
Air Force Material Command, USAF
Hanscom AFB, MA 01731-2816



Prepared by:

D. N. American
and
Electronic Warfare Associates, Inc.
under contract to
Unisys Corporation
12010 Sunrise Valley Drive
Reston, VA 22091

INFORMAL TECHNICAL REPORT
For The
SOFTWARE TECHNOLOGY FOR ADAPTABLE, RELIABLE SYSTEMS
(STARS)

Library Operations Policies and Procedures, Volume II
Central Archive for Reusable Defense Software
(CARDS)

STARS-VC-B004/002/01
28 February 1994

Data Type: Informal Technical Data

Contract NO. F19628-93-C-0130
Line Item 0002AB

Prepared for:

Electronic Systems Center
Air Force Material Command, USAF
Hanscom AFB, MA 01731-2816

Prepared by:

D. N. American
and
Electronic Warfare Associates, Inc.
under contract to
Unisys Corporation
12010 Sunrise Valley Drive
Reston, VA 22091

Data Reference: STARS-VC-B004/002/01
INFORMAL TECHNICAL REPORT
Library Operations Policies and Procedures, Volume II
Central Archive for Reusable Defense Software
(CARDS)

Distribution Statement "A"
per Dod Directive 5230.24
Approved for public release, distribution is unlimited

This document, developed under the Software Technology for Adaptable, Reliable Systems (STARS) program, is approved for release under Distribution "A" of the Scientific and Technical Information Program Classification Schema (DoD Directive 5230.24) unless otherwise indicated by the U.S. Sponsored by the U.S. Advanced Research Projects Agency (ARPA) under contract F19628-93-C-0130 the STARS program is supported by the military services with the U.S. Air Force as the executive contracting agent. The information identified herein is subject to change. For further information, contact the authors at the following mailer address: delivery@stars.reston.paramax.com

Data Reference: STARS-VC-B004/002/01
INFORMAL TECHNICAL REPORT
Library Operations Policies and Procedures, Volume II
Central Archive for Reusable Defense Software
(CARDS)

Principal Author(s):

Ricardo Cortes *Date*

Mark Quick *Date*

Approvals:

System Architect: *Kurt Wallnau* *Date*

Program Manager: *Lorraine Martin* *Date*

(Signatures on File)

Data Reference: STARS-VC-B004/002/01
INFORMAL TECHNICAL REPORT
Library Operations Policies and Procedures, Volume II
Central Archive for Reusable Defense Software
(CARDS)

ABSTRACT

The Central Archive for Reusable Defense Software (CARDS) Program is a DoD initiative to transfer the technologies of library-assisted, domain-specific reuse into other DoD software procedures and procurements. Volume Two of the Library Operation Policies and Procedures (LOPP) provides detailed operating instructions for day-to-day operation and maintenance of the Library.

Volume Two targets the technical individual who will be implementing the policies and procedures of the LOPP, Volume One. Volume Two provides detailed descriptions of the day-to-day tasks for operating and maintaining a reuse library. This document also provides quick access to the specific areas of interest and is designed to allow the reader to retrieve only information specific to their area of interest or concern. In addition to outlining the CARDS daily operations, Volume Two contains those forms referenced in Volume One.

Volume Two focuses on the CARDS Library as its model implementation environment. To allow the library implementor to use this document as a reference guide, Volume Two is intentionally organized to be free of a specific management structure.

REPORT DOCUMENTATON PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	28 February 1994	Final

4. TITLE AND SUBTITLE

Library Operations Policies and Procedures, Volume II

5. FUNDING NUMBERS

F19628-93-C-0130

6. AUTHOR(S)

Ricardo Cortes, Mark Quick

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Unisys Corporation
12010 Sunrise Valley Drive
Reston, VA 22091

8. PERFORMING ORGANIZATION REPORT NUMBER

STARS-VC-B004/002/01

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Department of the Air Force
ESC/ENS
Hanscom AFB, MA 01731-2816

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

B004

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT

DISTRIBUTION "A"

12 b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

The Central Archive for Reusable Defense Software (CARDS) Program is a DoD initiative to transfer the technologies of library-assisted, domain-specific reuse into other DoD software procedures and procurements. Volume Two of the Library Operation Policies and Procedures (LOPP) provides detailed operating instructions for day-to-day operation and maintenance of the Library.

Volume Two targets the technical individual who will be implementing the policies and procedures of the LOPP, Volume One. Volume Two provides detailed descriptions of the day-to-day tasks for operating and maintaining a reuse library. This document also provides quick access to the specific areas of interest and is designed to allow the reader to retrieve only information specific to their area of interest or concern. In addition to outlining the CARDS daily operations, Volume Two contains those forms referenced in Volume One.

Volume Two focuses on the CARDS Library as its model implementation environment. To allow the library implementor to use this document as a reference guide, Volume Two is intentionally organized to be free of a specific management structure.

14. SUBJECT TERMS

Management Structure, User Support, Computer Resources, Security, Quality Assurance, Configuration Management, Interoperability, Metrics

15. NUMBER OF PAGES

172

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAR

Table of Contents

1 INTRODUCTION

1.1 PURPOSE

This is the second volume of the Library Operations Policies and Procedures (LOPP) manual. This volume, Volume Two, provides detailed operating instructions for day-to-day operation and maintenance of the Library. Volume One outlines the recommended policies and procedures for library operations.

Volumes One and Two are partitioned to allow for maximum modularity and ease of use for the manual user. Volume One is aimed toward upper level management through the technical supervisor level and provides a high level view of the policies and procedures for the library operations. Volume One also provides access to information concerning strategies for managing and maintaining an existing reuse library system. This includes recommendations on how to implement operations of the Library, tables showing suggestions on how to assure task accountability and completion, and an expected skill set for the staff at hand.

Volume Two, Operating Instructions, targets the technical individual who will be implementing the policies and procedures of Volume One. The Operating Instructions provide detailed descriptions of the day-to-day tasks for implementing and maintaining a reuse library. Both volumes provide quick access to the specific areas of interest and are designed to allow the reader to retrieve only information specific to their area of interest or concern. In addition to outlining the Central Archive for Reusable Defense Software (CARDS) daily operations, Volume Two contains those forms referenced in Volume One.

1.2 SCOPE

This manual may be implemented by any domain oriented operational reuse library (referred to as "the Library"). Volume Two illustrates the day-to-day instructions implemented at the CARDS facility. These operating instructions support the policies and procedures outlined in Volume One.

Initial Library development, i.e., general Library start-up activities, are out of the scope of the LOPP. Information about Library start-up activities can be found in the Franchise Plan document [CARDS93b], the Library Development Handbook (LDH) [CARDS93d], and the Technical Concept Document (TCD) [CARDS93a].

The Library Operations Policies and Procedures manual was last published on 1 October 1993. This release is an update to Volume One, Policies and Procedures manual, and Volume Two, Operating Instructions, of the LOPP [CARDS94a][CARDS94b]. The updates in this release of Volume Two include revisions to the day-to-day instructions that reflect the current practices at the CARDS library.

This manual contains some evolving issues and open questions related to Library operating instructions. The dynamic nature of the Library necessitates continuous feed back and

refinements. Modifications to this manual will reflect the Library staff's increasing knowledge base.

1.3 BACKGROUND

The CARDS Program is a concerted DoD effort to transition advances in the techniques of domain-specific software reuse into mainstream DoD software procurements. This technology transition effort combines a concrete demonstration project to illustrate the potential of domain specific reuse - in this case for the domain of Command Centers (CC) - with a broad-scale attack on the cultural and contractual inhibitors to software reuse.

1.3.1 Relationship to Other Reuse Libraries

In domain oriented reuse libraries, the emphasis is placed on the components' complex relationships and how these relationships are used to generate applications which meet new and unique user requirements.

CARDS has established a domain oriented Library sponsored by the Air Force ESC/ENS. The CARDS effort utilizes, when appropriate, existing operating instructions from other programs such as the Asset Source for Software Engineering Technology (ASSET) and the Defense Information Systems Agency's (DISA) Defense Software Repository System (DSRS). CARDS also refers to the guidelines proposed by the Reuse library Interoperability Group (RIG).

Currendy CARDS has developed an operational library for the domain of Command Centers (CC). CARDS is planning to develop operational libraries for other domains.

1.3.2 Differentiation from Other Libraries

CARDS Command Center Library System Library adheres to a model-based paradigm in support of domain-specific reuse. Model-based libraries use domain models as a foundation for library organization and a framework for supporting applications which exploit these models to automate various library services.

The products of Domain Analysis are encoded into a Library Model. The Library Model also contains additional information such as Component Qualification Criteria. Additionally, the System LIbrary acquires and qualifies reusable components in support of the Library Model. Thus, CARDS provides value-added services to products of Domain Analysis.

Another distinction is realized through CARDS interoperability with other libraries. One of the goals of CARDS is to provide a consistent method of access to and from other relevant libraries, enabling reusable components from these other libraries to become integral parts of the overall System Library. CARDS is currently cooperating with ASSET and DISA/DSRS to develop interoperation capabilities. CARDS is also a participating member of the RIG. The RIG is a

consensus group composed of industry, government, and academic personnel that is developing standards for library interoperability.

1.4 ASSUMPTIONS AND CONSTRAINTS

This section describes some constraints and assumptions upon which the operating instructions of this manual are based.

User interaction with the CARDS Library occurs locally at the Library central site and from multiple remote access sites. Each remote access site has the same interface and functionality that is available at the Library central site in Fairmont, WV. CARDS users interact with the Unix operating system through a Unix shell interpreter. The Graphical Interface to the System Library is the Reusability Library Framework (RLF). The RLF is an X-Windows based tool which utilizes knowledge bases and semantic networks to represent generic architectures. The components of the Library are displayed within the generic architecture in a user friendly graphical browsing tool (RLF_GB). The tool was developed by Unisys for the Software Technology for Adaptable Reliable Systems (STARS) Program and is public domain. AFS is used as a distributed file system allowing the CARDS users to cache library files on their local machines. Once files are cached locally, the user should not experience the time delays in file access associated with remote computing.

Volume Two, Operating Instructions, does not address information regarding the reuse library start-up and development activities, nor the high level overview of policies and procedures for library operations. This volume is a detailed, flexible, modular, reusable guide for the day-to-day implementation, operation, and maintenance of a domain oriented software reuse library.

Volume Two assumes that the reader can log on to the system and is familiar with the systems' electronic mail tool. This manual uses the following conventions:

1. Command names, switches, and flags appear in bold type in syntax definitions, examples and running text.

2. Variable information appears in italic type. This includes user-supplied information on command lines and the parts of prompts that differ depending on who issues the command.

3. Names of directories volumes, files, file server machines and partitions appear in italic type.

4. New terms appear in ***bold italic type.***

5. Examples of screen output and file contents appear in type writer type (Courier font).

6. The following symbols appear in command syntax definitions, both in the manuals and online. When issuing a command, do not type any of these symbols:

- Square brackets [] surround optional items.
- Angle brackets <> surround instances (user-supplied information).
- A plus sign + follows an argument that accepts a list.
- A percent sign % represents the command shell prompt. Each system may employ a different prompt.

1.5 SUMMARY OF CONTENT

The format for each of the operating instructions in this manual follows a general outline. Each policy format contains a responsible role, supporting roles, frequency, preconditions, goal, related policies and a bibliography/references section.

The responsible role indicates the individual skill set having the ultimate accountability for the implementation of these operating instructions. The responsible role may not be listed as a performer of any of the operating instructions; however, this person effectively "owns" the policy.

The supporting roles show those roles that play a part in completing the operating instructions but are not the primarily responsible individuals. A list of the role titles is shown in Chapter Two, Management Structure and Description. This list indicates the skill set represented by a specific role.

Frequency is an indication of how often the operating instructions need to be executed. The precondition statement describes the user's and/or system's environment prior to the completion of this set of operating instructions. The goal indicates the resulting environment as a consequence of the operating instructions. Related policies list those policies and their section numbers which impact or are impacted by the current policies. The Bibliography/References section shows those documents used to write, implement, or support these operating instructions within a policy.

Chapter Two is a summary of the management structure that is in place at CARDS. This management structure is not necessarily the management structure that needs to be implemented at another library. Staff size, personnel capabilities, and existing management structure will affect the kind of management structure implemented at a library. The CARDS System Library management structure is, however, included for clarity and completeness.

As shown below, this manual provides the Operating Instructions for the specific areas indicated in chapters 3 through 9:

- Chapter 2 presents the Management Structure and Description that is currently in place at CARDS.
- Chapter 3 addresses User Support.

- Chapter 4 discusses Computer Resources.
- Chapter 5 examines Security.
- Chapter 6 covers Quality Assurance.
- Chapter 7 examines Configuration Management.
- Chapter 8 looks at Interoperability.
- Chapter 9 discusses Metrics.
- Appendix A shows a list of forms.
- Appendix B lists a Glossary.
- Appendix C list a Bibliography.

2 MANAGEMENT STRUCTURE AND DESCRIPTION

This Chapter describes the management structure and personnel relationships as envisioned by CARDS. The roles list and structure are intended to aid in the understanding of this manual for the CARDS library implementors. Another library may not desire to implement this management structure; however, it is included to give context to material contained in this manual.

The operating instructions contained within Chapters 3 through 9 indicate who is responsible for a particular process. This identification of a responsible individual is based on the CARDS Library roles defined in this Chapter. The purpose of defining roles is to allow a library implementor to use and customize those policies and procedures applicable to the implementor's situation. It is not the intent of this manual to restrict the library implementor by recommending a specific management or team structure. Modularity of the policies and procedures is increased to allow ease of customization for the library User or franchise.

A CARDS franchise is a partnership between a Government organization and CARDS to provide for technology transfer during the planning and implementation of the organization's software reuse initiative. Through a Memorandum of Understanding (MOU), which specifies the level of services, CARDS assists organizations in adopting a process-driven, domain-specific, architecture-centric, library-assisted software reuse capability. Bilateral technology transfer is achieved as CARDS and franchise engineers work side by side in joint reuse implementation efforts.

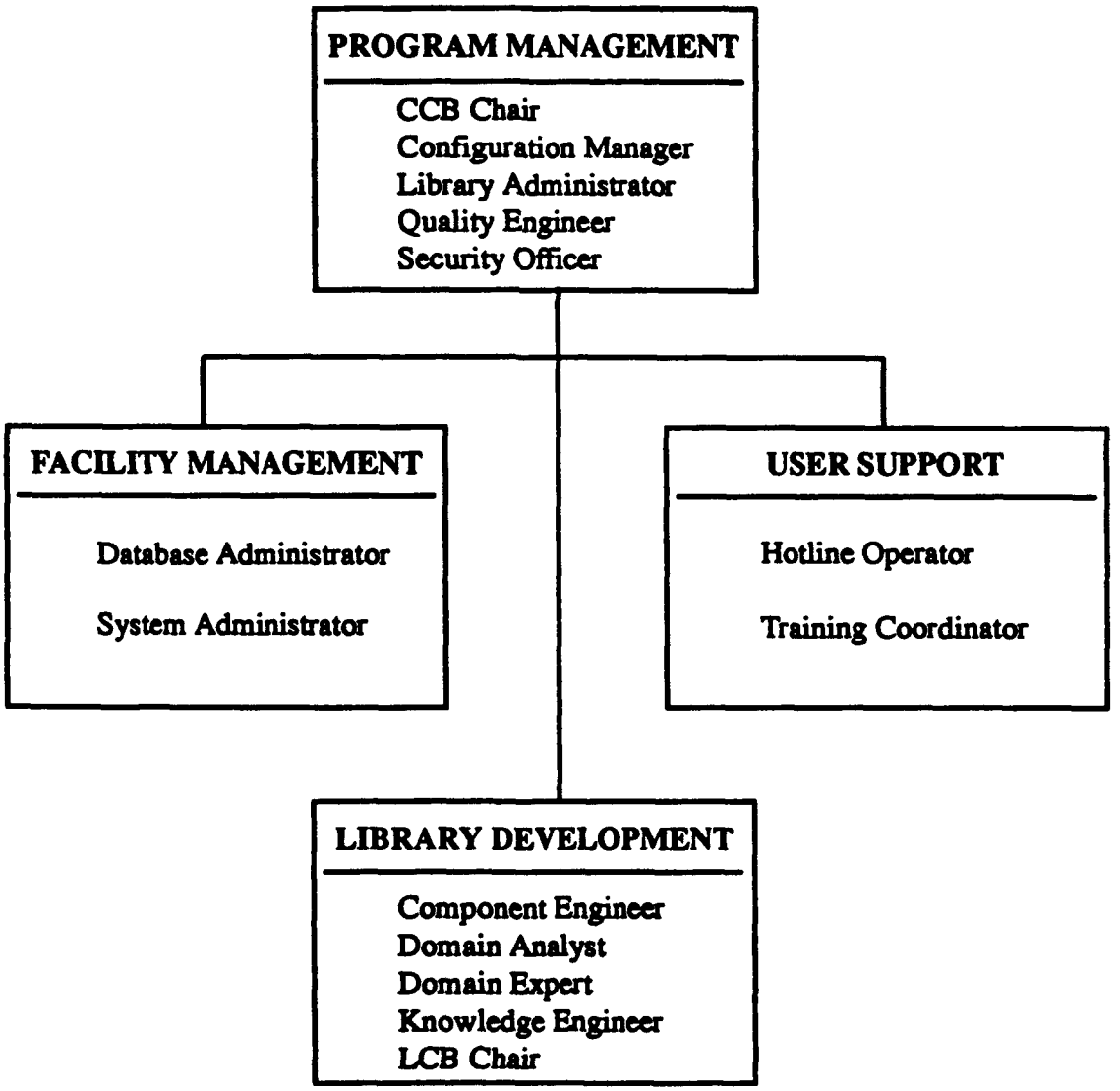
The management structure of the CARDS Library System encompasses the procedures for upper level management, staff, products, services, and facility. Figure 2-1 depicts the library management structure used for this LOPP. The purpose of this structure is to provide a LOPP baseline for discussion and to provide common terminology for organization names and job titles. This structure does not imply the way a library staff must be organized. After reading this LOPP, program management may want to modify this organizational structure to suit their mission and needs. Examples of possible Figure 2-1 changes include:

- Add job positions (e.g., staff positions such as accounting and finance).
- Delete job positions (e.g., Domain Engineer if another organization is responsible for this task).
- Modify job positions (e.g., Configuration Manager may also be the Configuration Control Board (CCB) Chairperson).
- Change the group organization (e.g., some job positions listed under Program Management and User Support could be placed into a group called 'Library Operations', i.e., maintain/run the operational library).

The intent of the LOPP management structure is as follows:

- Program Management: The job positions in this group provide support to the other groups to ensure the library meets the quality needs of the Users/customers. This group is also responsible for the operation of the library.

- Facility Management: The job positions in this group provide support to the library facility, e.g., database support, equipment (i.e., hardware and software) installation and maintenance, and overall computer and computer communications support.



- User Support: The job positions in this group provide support to the Users by acting as a liaison between the Staff and the library Users/customers. Examples of their support include receiving and logging User library problems and arranging and providing training on how to use the library.

- Library Development: The job positions in this group provide support to creating the library, i. e., a technical review board (Library Control Board - LCB). This group is similar to a software development group, but works on developing the library.

A list of library staff job positions/roles is provided in the next section. The number of people needed to fill each role will be driven by the size of the library (or "libraries"), skill and knowledge level of personnel, operational funding and schedule, availability of resources, and user demands.

ROLES OF LIBRARY STAFF

Account Holder -

An Account Holder/Library Account Holder is a person/group (e.g., Users or Library Staff) authorized access to one or more reuse library.

CCB Chair -

The CCB Chairperson is the point of contact for the Configuration Control Board (CCB). The CCB resolves all management level issues dealing with the operational libraries, e.g., operational hardware and software, and library operations. The CCB also approves or rejects operational model releases proposed by the Library Control Board (LCB). Decisions within the CCB are reflected through the CCB Chairperson.

Component Engineer -

The Component Engineer is responsible for evaluating library components, adapting the components if necessary, collecting metrics upon the components, analyzing the metrics, integrating components, and reporting the findings as appropriate.

Configuration Manager -

The configuration manager is responsible for overseeing proper Configuration Management (CM) of operational hardware and software, library models, library contents, and accompanying documentation. The Configuration Manager makes suggestions to the CCB and ensures that the CCB's library release decisions are implemented.

Database Administrator -

This person is responsible for maintaining the library support database. The database is used to store information about the operation of the library (e.g., metrics, Library Account Holder information, etc.). Responsibilities may include, but are not limited to: designing an appropriate structure for the database, maintaining proper data base CM, writing policies and procedures pertaining to the database, training personnel in the use of the database, and determining database access privileges.

Database Owner -

The Database Owner is a staff member who has ownership privileges to a supported database. The Database Owner is responsible for giving database users access to the owned database, and for granting and revoking certain permissions to database users.

Domain Analyst -

The Domain Analyst is an individual skilled in domain analysis methodologies. This person provides the procedural know-how on domain analysis. The Domain Analyst is responsible for defining the language, tools, and techniques to be used in performing the domain analysis. This person also documents the domain model and may be responsible for defining any generic architectures associated with the domain. This person is generally responsible for training personnel in the use of the domain analysis methodology, assessing conformance to any applicable standards and procedures, and providing expertise in the area of systems/software engineering.

Domain Expert -

The Domain Expert is an individual with extensive knowledge of the application domain being examined. This person acts as a consultant to other domain analysis personnel, assists in defining model(s) of the domain, finding and analyzing existing systems, anticipating and assessing the impact of future system requirements, and acts as a consultant to systems development personnel building new application systems in the domain.

Hotline Operator -

The Hotline Operator is the user's main library point of contact. The Hotline Operator takes requests, questions, problems, and comments from users over the phone and by e-mail. The Hotline Operator resolves user requests at that time if possible. This person is responsible for tracking this information throughout the resolution process and forwarding it to the Library Administrator. The Hotline Operator is also responsible for collecting related user metrics.

Knowledge Engineer -

This person is responsible for modeling domains. The Knowledge Engineer works closely with the Domain Analyst and the Domain Expert in defining the scope of a reuse library domain. The Knowledge Engineer is the point of contact for problems with the library model, develops changes to be implemented in the library model, and documents changes to the library model.

Library Account Holder -

See Account Holder

Library Administrator -

The Library Administrator is responsible for maintaining user satisfaction of the library. This person receives user requests from the Hotline Operator and forwards these requests to appropriate Staff for resolution. The Library Administrator makes proposals to the CCB for upgrading user services as well as proposals involving operational hardware, software, policies, and procedures. This person is also responsible for briefing the CCB about any unresolved hotline requests. This person has overall management and technical responsibility for the library architecture and operations.

Library Control Board (LCB) Chair -

The LCB Chairperson is the point of contact for the LCB. The LCB resolves problems dealing with technical issues (e.g., components and system tools) within the library models. The LCB examines model releases developed by library development personnel and new library tools and either rejects them, requests modification to them, authorizes implementation, or proposes them to the CCB. Decisions within the LCB are reflected through the LCB Chairperson and LCB minutes.

Library Developer -

A Library Developer works on the developmental libraries and their contents. Developmental libraries, after approval of the LCB and CCB, become Operational Libraries. Library Developers qualify components for the libraries, develop library tools, and analyze and repair most library problems.

Quality Engineer -

A Quality Engineer is the person responsible for monitoring Total Quality Management (TQM) at the library facility. This person is responsible for implementing 'quality' policies and procedures, writing these policies and procedures into the policies and procedures manual, providing review of products and procedures, providing reports on the progress of TQM within the library, and recommending improvements.

Release Manager

The Release Manager provides franchisees with media copies of existing libraries, as needed.

Security Officer -

The Security Officer is responsible for, but not limited to: being the library point of contact for all matters relating to library security; coordinating the preparation of security plans, reports, policies, and procedures; preparing and conducting periodic security audits and reviews (e.g., during library releases); preparing monthly security reports; and providing security training and consultation to library staff, users, library implementors, and potential library franchisees.

Security Team

The Security Team assists the Security Officer with security analysis. Team members are knowledgeable in all aspects of library operation and security, and provide different viewpoints.

Staff -

A Staff member is anyone (but not a User) working at the library, e.g., Library Developer. This individual's duties include functions related to operating and maintaining a library, such as problem resolution, administrative, etc.

System Administrator -

The System Administrator performs facility management tasks including, but not limited to: system operations, installing, testing and maintaining system hardware and software, conducting system security audits, installing new accounts, management of system software, collecting system metrics data, conducting system backups, and conducting correspondence with hardware and software vendors.

Training Coordinator -

This person is responsible for all training. The Training Coordinator arranges training for new staff, users, and franchise organizations, evaluates and provides updates to the training materials, selects and evaluates training instructors, and coordinates and tailors training for franchise organizations.

3 USER SUPPORT

User Support is responsible for developing and maintaining a bi-directional interface with established and potential Library Account Holders, and for ensuring that Library Account Holders are satisfied with Library operations. All Library processes and activities support the Library Account Holder. User Support is a focal point between these processes and the Library Account Holder.

User Support encompasses all functions related to the administrative support of the Library Account Holder. To maintain continuity and provide a central point of contact between the Library Staff and Library Account Holders, User Support operates a Library Hotline. User Support ensures all requests and queries of established Library Account Holders are addressed and resolved by interacting with Library Staff and tracking Hotline Reports throughout the resolution process. The Hotline provides potential Library Users and Library Customers with information about Library activities and capabilities.

User Support monitors account activity, gathers metrics, establishes and maintains accounts and account information, and collects user feedback on library operations. User Support also is responsible for the preparation of educational materials and for scheduling training sessions.

This Chapter, User Support, outlines detailed Operating Instructions which are provided as an example of how CARDS User Support implements policies and procedures in the day-to-day operations of the CARDS Library. Frequently used User Support forms are included as sample templates for those who may wish to develop similar User Support documentation procedures when implementing a library (See Appendix A).

In Volume One, the User Support chapter outlines administrative policies and procedures in the following sections: Managing Library Accounts, Terminating Library Accounts, Resolving Hotline Requests, Updating and Notifying Account Holders, Training Account Holders, and Maintaining Hotline Documentation.

These policies and procedures directly involve the Library Administrator, the Hotline Operator, and the Training Coordinator; however, all staff involved in Library operations should become familiar with these guidelines to effectively support Library Account Holders.

3.1 MANAGING LIBRARY ACCOUNTS

3.1.1 Establishing a Library Account

Responsible Role: Hotline Operator

Supporting Role(s): System Administrator, Library Administrator

1. Frequency

   As needed.

2. Preconditions

   For a Library Account to be established, an individual must request a Library Account.

3. Goal

   The goal of this procedure is to show how to establish a Library Account.

4. Operating Instructions

   A. An individual contacts the CARDS Hotline in some manner (i.e., phone, fax, e-mail, surface mail) with a request for a Library account.

   B. If the individual requests a CARDS Library account, the Hotline Operator sends the potential User a Registration Packet. Currently, the Registration Packet includes a CARDS Library Account Registration Form (CLARF), a CARDS Library Account Holder Rights and Responsibilities Statement (CLAHRRS), and a listing of minimum hardware and software requirements needed to access the CARDS Library from a remote site. This information is recorded on the CARDS Requests Log.

      An example of the CLARF, previously referred to as the User Registration Form (URF), is included in Chapter 10. An example of the CLAHRRS is located in *LOPP Volume One, 5.4 User Rights and Responsibilities.*

   C. The individual completes a CLARF (and becomes a User Recruit), and returns the original CLARF to the Hotline Operator via surface mail. The Hotline Operator verifies that the CLARF is complete, i.e., when the applicant provides all information required on the CLARF, including acknowledgment that the individual has read the User Rights and Responsibilities Statement. The Hotline Operator must receive the original CLARF so that original signatures can be kept on file.

   D. If the CLARF is not completed, the Hotline Operator returns the original CLARF to the User Recruit via surface mail, along with a cover letter requesting specific information which the applicant needs to provide. This is noted in the CARDS Account Activation Log.

   E. The Hotline Operator attaches a final authorization sheet to the CLARF and stamps the CLARF in the upper right hand corner with the date of receipt. An example of the final authorization sheet is located in Chapter 10.

   F. The Account must then be approved for activation. An appropriate management authority approves or disapproves account activation, account type and access

privileges (such as AFS subdirectories and UNIX mail alias groups), and signs and dates the CLARF. Depending on the type of account, an appropriate management authority may be the CARDS Program Manager, the Program Manager's representative, or the Library Administrator.

G. There are two basic Library Account types: Staff accounts and User accounts. These basic types of accounts are further categorized based on access privileges and resource hardware/software configuration. Currently, the CARDS Library System has five types of accounts.

There are two types of Staff Accounts:

- **Staff Developer** Accounts require highest level access privileges and are currently used by members of the Library Development Team.
- **Staff** Accounts are for all other Library Staff members.

There are two types of Accounts for Users:

- Users **with** Sun4 workstations and AFS
- Users **without** Sun4 workstations or without AFS

There is also another type of account for management level personnel:

- **Staff Affiliate** Accounts are similar to Staff Accounts, except with restricted access privileges. Currently, Staff Affiliates are not included in the cards-team alias group.

H. In most cases, a CARDS Library Account is approved. Government employees or individuals working on a government contract may be Library Account Holders. Any exceptions must be approved by program management. Another reason for disapproval may be security considerations. For the most part, a CARDS Library account may be disapproved for the following reasons:

- The User Recruit has previously been a CARDS Library Account Holder whose Library Account was terminated on the grounds of misuse;
- The User Recruit wishes to use the Library Account for purposes other than those in the User Rights and Responsibilities Statement.

I. If account activation is not approved:

The Hotline Operator notifies the User Recruit of disapproval and reason(s) for disapproval via phone and a Rejection of Account Letter.

J. If the new account is approved:

The Hotline Operator creates a physical file folder for the CLARF and submits the original CLARF to the System Administrator for account activation. In the CARDS Account Activation Log, the Hotline Operator records the date of approval and submission to the System Administrator.

K. The System Administrator activates and tests the account, and records the following information on the authorization sheet of the original CLARF:

- Unix Account Name
- Date of Activation
- Unix User ID
- Initial Unix Password
- AFS Account Name
- Date of Activation
- AFS User ID
- Initial AFS Password

L. The System Administrator tests the account by checking the functionality of basic operational functions. The testing procedures will vary, depending on the type of account.

M. The System Administrator returns the CLARF to the Hotline Operator.

N. The Hotline Operator records, in the CARDS Account Activation Log, the date of account activation and the date that the CLARF is returned from the System Administrator.

O. The Hotline Operator forwards the CLARF to the Staff Developer in charge of the Interoperability Server List. The Staff Developer adds the user's AFS account name and distribution status ("C" = Government, "A" = Public Domain) to the list.

P. The Staff Developer returns the CLARF to the Hotline Operator.

Q. The Hotline Operator records, in the CARDS Account Activation Log, the date the user is added to the Interoperability Server's List.

R. The Hotline Operator adds the new Library Account Holder to the appropriated mail alias group.

S. The Hotline Operator notifies the Library Account Holder of account activation by phone, and gives the Library Account Holder any necessary passwords (UNIX and AFS). The date of notification is recorded in the CARDS Account Activation Log.

T. The Hotline Operator sends the new Library Account Holder the Remote Login Procedures, the location of CARDS documentation in an AFS directory such as /afs/cards/Library/DoneDocs, and current library release information.

U. The original hard-copy CLARF is kept under file in the CLARF Folder at the Hotline Operator's location.

5. Related Policies

   3.1.2 Reactivating a Library Account

   3.1.3 Updating a Library Account

   3.6 MAINTAINING HOTLINE DOCUMENTATION

6. Bibliography

   None

3.1.2 Reactivating a Library Account

Responsible Role: Hotline Operator

Supporting Role(s): System Administrator, Library Administrator

1. Frequency

   As needed.

2. Preconditions

   For a Library Account to be reactivated, an individual must request that a terminated account be reactivated.

3. Goal

   The goal is to reactivate the Library account in a timely manner.

4. Operating Instructions

   A. Account renewal is the reactivation of a terminated Library Account. To renew a Library Account, the former Account Holder, like a new applicant, must repeat the process for establishing a new Account as outlined in 3.1.1 Establishing a Library Account.

5. Related Policies

   3.1.1 Establishing a Library Account

   3.6 MAINTAINING HOTLINE DOCUMENTATION

6. Bibliography

   None

3.1.3 Updating a Library Account

Responsible Role: Hotline Operator

Supporting Role(s): System Administrator, Library Administrator

1. Frequency

   As needed.

2. Preconditions

   For a Library Account to be updated, a Library Account Holder must request that the Account be updated.

3. Goal

   The goal is to update the Library Account in a timely manner.

4. Operating Instructions

   A. Library Account Holders are required to notify the Hotline of any change in status, such as: Name, Address, Telephone Number, Company/Agency, Government Contract, and new Hardware.

   B. The Account Holder notifies the Hotline of any status changes or updates.

   C. The Hotline Operator sends, via surface mail, a new CLARF to the Account Holder for completion.

D. The Account Holder completes, signs, and returns the new CLARF to the Hotline.

E. The Hotline Operator enters the date of receipt into the CARDS Account Activation Log.

F. If necessary, the Hotline Operator submits the CLARF to the System Administrator for Library Account update. The System Administrator returns the CLARF to the Hotline Operator after making any Library Account changes.

G. The Hotline Operator records any updated account information in the CARDS Account Activation Log.

5. Related Policies

   3.1.1 Establishing a Library Account

   3.6 MAINTAINING HOTLINE DOCUMENTATION

6. Bibliography

   None

3.2 TERMINATING A LIBRARY ACCOUNT

Responsible Role: Hotline Operator

Supporting Role(s): System Administrator, Library Administrator

1. Frequency

   As needed.

2. Preconditions

   The System Administrator checks Library Accounts periodically (monthly) to identify inactive accounts and then coordinates with the Hotline Operator to determine if Account termination is necessary. Library Accounts which have not been accessed for six months are considered inactive and may be terminated.

   Library Accounts may be terminated at the Account Holder's request. If the Account Holder no longer requires access to the Library, the Account Holder must notify the Hotline.

   If Possible, Library Account Holders are contacted by the Hotline Operator before Library Account termination. In the case of Library Account Holders who have not accessed their Library Account for six months:

- If status is unchanged and the Library Account Holder wishes to keep the Account, the Library Account remains.

- If the user has resigned from the organization, or no longer qualifies for a Library Account, the Library Account is terminated.

- If the Library Account Holder violates the conditions of the User Rights and Responsibilities Statement by using a Library Account for unauthorized purposes, the Library Account is terminated. Currently, appropriate management personnel determine if an account is used for unauthorized purposes. Appropriate management personnel could include the Program Manager, Program Manager's representative, Library Administrator, or Security Officer.

1. Goal

   The goal of this procedure is to terminate the Library Account.

2. Operating Instructions

   A. The Hotline Operator contacts the Library Account Holder to verify that the account is to be terminated.

   B. If the Library Account is to be terminated, the Hotline Operator submits the CLARF to the System Administrator for account termination.

   C. The System Administrator terminates the account, records the date of termination on the last page of the CLARF, and returns the CLARF to the Hotline Operator.

   D. The Hotline Operator records the date of termination in the CARDS Account Deactivation Log.

   E. The Hotline Operator notifies the Library Account Holder, via surface mail, that the Library Account has been terminated, if possible.

3. Related Policies

   3.1 MANAGING LIBRARY ACCOUNTS

   3.6 MAINTAINING HOTLINE DOCUMENTATION

4. Bibliography

   None

3.3 RESOLVING HOTLINE REQUESTS

3.3.1 Overview

The CARDS Hotline Operator deals primarily with two categories of callers: Library Account Holders (Users and Staff), and others. Others include Potential Users, User Recruits, Potential Customers, Customers and Franchisees. A Potential User is an individual who requests a Library Account. A User Recruit has been sent a CARDS Library Account Registration Form (CLARF), a CARDS Library Account Holder Rights and Responsibilities statement, and CARDS Remote User Site Configuration List by the Hotline Operator. A Potential Customer is an individual who requests information about products and/or services from CARDS. A Customer is an individual who has received CARDS products and services. A Franchisee has a memorandum of understanding (MOU) with CARDS, and is interested in developing a domain-specific reuse infrastructure.

If the Hotline Operator is unable to immediately resolve a caller's request, the expertise of the entire CARDS Staff is available to resolve the request. This requires distribution of a detailed explanation of the request to an appropriate individual or individuals.

To effectively track a request while in the resolution process, three types of reports may be used: User Hotline Reports, Staff Hotline Report, or Staff Work Order, all of which originate from the CARDS Hotline.

Hotline Reports

User Hotline Reports and Staff Hotline Reports ensure that a Library Account Holder's issue is resolved. Hotline Reports are used to track a Library Account Holder's issue while in the resolution process and to document the steps of the resolution process itself. Hotline Reports are also used for reference in resolving other Library Account Holder's issues and for metrics to evaluate CARDS products and processes, and the level of satisfaction.

Informational requests are from callers, typically Potential Users and Potential Customers, who desire information about the CARDS Library System or the CARDS Program. The Hotline Operator fulfills these requests by sending the caller, via surface mail, CARDS documentation, an Information Packet, a User Recruit Packet, or a CARDS Component Packet. These packets are outlined in 3.1 Managing Library Accounts. Requests for such information are common and are not tracked as Hotline Reports. These requests are logged and maintained in a separate file according to the individual requestor's name. Other informational requests may be referred to appropriate Staff members.

Since informational requests are usually easily handled and not difficult to resolve, they are addressed only below.

REQUESTS FOR INFORMATION ABOUT THE CARDS PROGRAM. If the Potential Customer requests general information about CARDS, the Hotline Operator sends the individual an Information Packet via surface mail. Currently, the Information Packet includes a cover letter, the CARDS brochure, an article about CARDS (reprinted from trade publication), and a

promotional flyer/pamphlet. The cover letter instructs the individual to contact the Hotline if further information or services are desired. If the Potential Customer requests specific, detailed information about CARDS, the Hotline Operator answers these questions. If the Hotline Operator is unable to answer these questions, the request is handled by appropriate management personnel as determined by the Hotline Operator. Appropriate management personnel could include the Program Manager, Technical Architect, and so forth.

REQUESTS FOR INFORMATION ABOUT A CARDS LIBRARY. If the Potential User requests general information about a CARDS Library, the Hotline Operator sends the Potential User an Information Packet via surface mail. The Information Packet includes a cover letter, two articles about CARDS (reprinted from trade publications), and a promotional flyer/pamphlet. Depending on the level of detail the User or Potential User desires, the CARDS Component Packet also provides information concerning the CARDS Libraries. The CARDS Component Packet includes a cover letter, the CARDS Command Center Library Contents and Status Report, the CARDS Command Center Library Submittal Guidelines, and articles written by the CARDS Staff. The cover letter, contained in each packet, instructs the individual to contact the Hotline if further information or services are desired.

Unstaffed Hotline Position

In the unlikely occurrence that the Hotline is unstaffed, the Hotline Operator uses an answering machine to record all incoming phone calls. If possible, the Library Administrator or authorized representative checks the answering machine and the Hotline e-mail account hourly, and returns any calls or messages as needed.

3.3.2 Hotline Operations Procedures

Responsible Role: Library Administrator

Supporting Role(s): Hotline Operator, System Administrator, Library Staff

1. Frequency

   As needed.

2. Preconditions

   A request comes to the Hotline Operator for resolution.

3. Goal

   The goal of the CARDS Hotline is to promptly fulfill the requests of callers.

4. Operating Instructions

   A. The Hotline Operator receives a Hotline Request by e-mail, telephone, or hard-copy from a CARDS Library Account Holder.

B. The Hotline Operator classifies the caller as either:

- A Library User, or
- A Library Staff member

C. The current date and time of the report is immediately recorded in the Hotline Correspondence Log.

D. The Hotline Operator determines whether or not the User's request requires a Hotline Report. If so, the date is recorded on the Hotline Report. If the Hotline Request is by telephone, the Hotline Operator gathers and records detailed information, as required in the Hotline Report. If the Hotline Request is received via e-mail, the Hotline Operator copies the entire message into the on-line Hotline Report.

E. If necessary, the Hotline Operator cross references and confirms/verifies the CARDS Library Account Holder's information with the details supplied on the CARDS Account Holder's current Registration Form (CLARF), which is filed in the CLARF Folder. If the Hotline Request is by telephone, the Hotline Operator may identify the CARDS Library Account Holder using the Unique Identification Information described on the CLARF.

F. If a CARDS Library Account Holder asks for a specific CARDS Staff member, the Hotline Operator provides the office telephone number for the Staff member, or takes a message from the Account Holder, to include a phone number, so that the Staff member may return the call as soon as possible.

G. The Hotline Operator defines the nature of the request by collecting and recording specific information in accordance with the Hotline Report. The Hotline Operator also defines the category of the request (such as hardware, operational software, or components) and the priority level of the request.

H. The Hotline Operator uses subjective reasoning in assigning a priority level to a Hotline request. The severity and urgency of the request and Staff availability are factors affecting the priority level. For example, inability to access the system would be assigned high priority, as would a suspected virus. A change in mail alias group would be lower priority. As CARDS Library processes become more refined, a formal priority system will be developed.

I. The Hotline Operator collects as much information as necessary to gain an adequate response. This keeps both the Hotline Operator and the CARDS Staff member from unnecessarily contacting the CARDS Library Account Holder by calling back for more information.

J. The Hotline Operator assigns a Hotline Report Number to the Hotline Report. The Hotline Report Number is comprised of a one letter abbreviation (P for Potential User, C for Customer, U for User, S for Staff, and F for Franchisee), the current Julian date, either the account name for User/Staff or the last name for customer, and a running number of total Hotline Requests for that CARDS Library Account Holder. The running number of requests is obtained from the Resolved Issues Log or the Hotline Log.

K. For example, CARDS User Pat Doe sends an e-mail request to the CARDS Hotline on 1 February 1993. It is Pat Doe's fifth Hotline request. The Hotline Report Number is: U-03293-doe-05.

L. If the Hotline Operator is unable to fulfill the CARDS Library Account Holder's request immediately, the Hotline Operator, after informing the caller that the request will be resolved as soon as possible and ending the call, refers to the Hotline Report (open/resolved issues) Log for prior similar reports in an attempt to fulfill the Account Holder's request. If a similar request has been previously resolved, the Hotline Operator fulfills the Library Account Holder's request by following the step-by-step resolution instructions of an existing Hotline Report.

M. If the Hotline Operator is unable to satisfy the CARDS Library Account Holder's request after exhausting the available research materials, the Hotline Operator e-mails a copy of the on-line Hotline Report to the most qualified Staff member for resolution.

Table 3-1

Issue	Possible Initial Points of Contact
Hardware	Configuration Manager
Operational Software	Configuration Manager or System Administrator
Account Access	System Administrator
Components	Component Engineer
User Support	Library Administrator
Policy	Configuration Control Board (CCB)
Other	Library Administrator

N. Upon receipt of the Hotline Report, the Staff member confirms that he or she is qualified to address and resolve the request.

O. If the Staff member is unable to fulfill the CARDS Library Account Holder's request, the Hotline Operator and the Staff member coordinate efforts to further

identify a qualified Staff member. In some cases, more than one individual Staff member may be required.

P. The Staff member provides an estimated time of resolution for the Hotline Request and provides that information to the Hotline Operator.

Q. Within one hour of receipt of the CARDS Library Account Holder's request, the Hotline Operator transmits an acknowledgment Message to the Account Holder. If the Staff member provides the Hotline Operator with an estimated time of resolution within the one hour time period, the Hotline Operator sends the Account Holder a detailed acknowledgment Message indicating the estimated time of resolution.

R. If the Staff member does not provide the Hotline Operator with an estimated time of resolution within one hour of request receipt, the Hotline Operator sends the CARDS Library Account Holder a general acknowledgment Message. As soon as possible, but within three business days of receipt of the original request, the Hotline Operator notifies the Account Holder of the estimated time of resolution.

S. All Hotline Reports are reviewed weekly by the Hotline Operator and the Library Administrator. At that time, if a Hotline Report remains unanswered beyond the estimated date of resolution, the Hotline Operator contacts the Staff member resolving the request to determine the status of the open issue. The Staff member responds, via phone or e-mail, to the Hotline Operator reporting the steps already completed in responding to the CARDS Library Account Holder's request, and also provides an updated estimated time of resolution.

T. The Hotline Operator transmits the information to the CARDS Library Account Holder, via phone or e-mail, in a follow-up call. The Hotline Operator provides the Account Holder with an updated time of resolution. If necessary, the Hotline Operator provides the Library Account Holder with status information every three business days at maximum until the request is answered. The contact with the Account Holder is recorded in the Hotline Correspondence Log.

U. Steps R, S, and T are repeated until the CARDS Library Account Holder's request is fulfilled.

V. The Staff member fulfills the request of the CARDS Library Account Holder and documents the resolution steps on the Hotline Report.

W. The Staff member notifies the Hotline Operator that the CARDS Library Account Holder's request is answered and returns the Hotline Report, via e-mail, to the Hotline Operator.

X. The Hotline Operator sends the CARDS Library Account Holder a Resolution Letter via e-mail, which contains a copy of the Library Account Holder's original e-mail message or a summary of the Library Account Holder's phone request, and a detailed response to the Library Account Holder's request. The original Hotline Report is maintained on-line for future reference.

5. Related Policies

   3.1 MANAGING LIBRARY ACCOUNTS

   3.6 MAINTAINING HOTLINE DOCUMENTATION

6. Bibliography

   None

3.4 UPDATING AND NOTIFYING CARDS LIBRARY ACCOUNT HOLDERS

Responsible Role: Library Administrator

Supporting Role(s): Hotline Operator

1. Frequency

   As needed.

2. Preconditions

   Information must be relayed to the Library Administrator.

3. Goal

   The goal is to relay information to CARDS Library Account Holders from a central point of contact.

4. Operating Instructions

   A. Information to be relayed to CARDS Library Account Holders is presented to the Library Administrator. This information may be version releases of software, changes in procedures, scheduled system downtime, archive and backup schedules, new additions to the Library, and so forth. This information may be presented to the Library Administrator by Staff members, CCB members, etc.

   B. The Library Administrator organizes this information for release to CARDS Library Account Holders by hard-copy media release or by e-mail update. Hard-copy media may include Newsletters, pamphlets/flyers, etc. Currently CARDS has released a promotional flyer CARDS and the CARDS Library. The

Library Administrator provides this information to the Hotline Operator. The Hotline Operator distributes this information to Library Account Holders via electronic or surface mail.

5. Related Policies

None

6. Bibliography

None

3.5 TRAINING CARDS LIBRARY ACCOUNT HOLDERS

Responsible Role: Training Coordinator

Supporting Role(s): Hotline Operator, Library Administrator

1. Frequency

Training for CARDS Library Account Holders occurs when the Library Account is established.

Training for CARDS Library Staff occurs when the individual joins the CARDS Library Staff, and periodically.

2. Preconditions

New CARDS Library Account Holders and new Library Staff require training.

3. Goal

The goal of training is to provide the CARDS Library Account Holder and Staff with the minimum skills needed to effectively utilize the CARDS Library.

4. Operating Instructions

A. Currently when a CARDS Library account is activated, the Hotline Operator provides the CARDS Library Account Holder with access to a Library User's Guide and an RLF-GB Manual.

B. Periodically, there are staff training sessions on topics such as the Hotline, X-Windows, Sybase, the RLF-GB, and basic system functions such as e-mail.

C. This section will be updated as CARDS training develops in the future.

5. Related Policies

None

6. Bibliography

None

3.6 MAINTAINING HOTLINE DOCUMENTATION

Responsible Role: Hotline Operator

Supporting Role(s): System Administrator, Library Administrator, Library Staff

1. Frequency

Continually.

2. Preconditions

The Hotline Operator uses a variety of forms in performing administrative duties, managing the Hotline and in corresponding with CARDS Library Account Holders. The conditions which dictate utilization of these forms are also discussed in sections 3.1 Managing Library Accounts, 3.2 Terminating Library Accounts, and 3.3 Resolving Hotline Requests.

3. Goal

The goal of this procedure is to initiate, organize, and effectively maintain Hotline documentation to maximize service to CARDS Library Account Holders.

4. Operating Instructions

A. The Hotline Correspondence Log is used to document all incoming and outgoing Hotline calls.

B. The CARDS Library Account Registration Form (CLARF) is the application for establishing a CARDS Library Account. The CLARF contains CARDS Library Account Holder supplied information (such as system configuration, personal contact information, and authorizing signatures), and administrative information (such as date of account activation and e-mail address).

C. The CLARF Authorization Sheet is an administrative form which designates the applicant's appropriate mail alias group and contains the required approval signatures for activation of the applicant's CLARF.

D. The CLARF Folder is a binder containing the original CLARF.

E. The CARDS Account Activation Log tracks each step of the account activation process.

F. The CARDS Account Deactivation Log tracks each step of the account deactivation process.

G. The CARDS Request Log tracks the types of information each user requests. Examples of such information includes: the Information Packet, the User Recruit Packet, the Component Packet, and CARDS documentation.

H. The Hotline Report is used to track a Hotline Request throughout the resolution process.

I. The Hotline Report Log is an administrative form which logs all current open issues and previously resolved Hotline Reports.

J. The Staff Work Order (SWO) is used to track a staff members request throughout the resolution process.

K. The SWOs Log is an administrative form which logs all current open issues and previously resolved Staff Work Orders.

L. A database may be used to store Hotline documentation forms. Plans also include a formal priority system for Hotline Reports.

M. The Hotline Operator is responsible for three packets: the Information Packet, the User Recruit Packet, and the Component Packet. These are discussed in section 3.3, Resolving Hotline Requests.

N. There are several form letters which the Hotline Operator routinely uses. The Request for Information Letter is sent to applicants who need to supply more information on the original CLARF before a library account can be established. The Rejection of Account Letter is used when an applicant is denied a library account, and the Termination of Account Letter is sent to a CARDS Library Account Holder when the library account is terminated. These are standard business form letters, and are not included in this document.

O. There are also form letters used in connection with Hotline Reports. These are the Acknowledgment Message, the Resolution Message, and the Follow-Up Message; they are standard business form letters, and are not included in this document.

5. Related Policies

4 COMPUTER RESOURCES

This chapter defines the operating instructions used in the daily system administration of the computer resources in a software library. Areas that fall under this chapter include hardware and software installation and maintenance, user and staff account maintenance and backup and restoration procedures.

4.1 SOFTWARE INSTALLATION AND UPGRADE

4.1.1 Software Installation and Upgrade procedure

Responsible Role: System Administrator

Supporting Role: CCB (Configuration Control Board), CM (Configuration Management)

1. Frequency

   Software will be installed as needed.

2. Preconditions

   Software installation may require approval by the CCB.

3. Goal

   Install software.

4. Operating Instructions

   A. Receive the installation/upgrade work order from the Library Administrator.

   B. Determine the impact of the installation/upgrade request on the Library system.

   C. If the installation/upgrade request may have an adverse effect on the Library system, inform the CCB via the Library Administrator.

   D. Read the package documentation.

   E. Determine the amount of disk space required to install the software package.

   F. Before installation/upgrade, perform the necessary backups.

   G. Physically install the software in the location that was predetermined by the CCB and log appropriate information.

   H. Test the effects of the actions taken.

   I. If no problems are encountered, inform the Library Administrator that the installation/upgrade request was completed.

   J. Complete the Operational Software Release Form.

K. If problems are encountered, inform the Library Administrator of the status of the installation/upgrade request.

5. Related Policies

None

6. Bibliography

System Administration 4.1.2 Student Guide, Sun Microsystems

4.1.2 Workorders procedure

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

Work orders will be processed as needed.

2. Preconditions

The work order must be within the scope of the System Administrator.

3. Goal

The goal in fulfilling a work order from an administrative perspective is to perform a request from a User in a manner that satisfies their request and has no adverse effects on the system.

4. Operating Instructions

A. Receive the work order from the Library Administrator.

B. Determine the impact of the request on the Library system.

C. Process the work order.

5. Related Policies

6. Bibliography

System Administration 4.1.2 Student Guide, Sun Microsystems

4.2 HARDWARE INSTALLATION AND MAINTENANCE

4.2.1 Workstation Firmware Protection

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

   The EEPROM password will be set on all new machines. The EEPROM password will be changed as needed.

2. Preconditions

   Be certain to choose a password that will not be forgotten but one that will be difficult for others to guess.

3. Goal

   To improve security by preventing the booting of a machine into any mode except multi-user mode.

4. Operating Instructions

   1. As root, type "eeprom" to check security-mode. If "security-mode=command" not displayed then type "eeprom security-mode=command".

   2. Set security password.

5. Related Policies

   None

6. Bibliography

   System Administration 4.1.2 Student Guide, Sun Microsystems

4.2.2 Workstation Installation

4.2.2.1 Adding a Diskless Client to a Server

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

Diskless clients will be added as needed.

2. Preconditions

   This is a complex operation and should be done in the presence of an experienced Unix administrator. If the hardware installation requires system down time, be certain that users have had adequate warning.

3. Goal

   The goal is to install a fully functional workstation without incurring the extra cost of purchasing a hard drive for it.

4. Operating Instructions

   A. Choose a machine that was configured to be a server. Check the size of your "d", "/export", and "e", "/export/swap" partitions to make sure they are large enough to support a diskless client. Use the df command to check the sizes.

   B. On your server, add the client to the "/etc/ethers" and "/etc/hosts" file.

      Example ethers file:
      hostname 8:0:20:9:0:85

   C. The ethers address is found by executing the dmesg command. The address is found in the resulting boot up messages.

      Example hosts file:
      192.9.200.25 hostname

   D. Add the client using the add_client program. Select none for your NIS type. Use a swap size appropriate to your /export/swap partition.

      Example Command Line:
      [hostname]# add_client -i

   E. Run ps -ax . From the command's display, confirm that you have the appropriate daemons running (rarpd and rpc.bootparamd) to support diskless clients.

   F. Once the file server steps are complete, boot the diskless client across the network using the appropriate boot PROM command below:

      ok boot net > b le()
      ok boot > b
      ok boot le()

5. Related Policies

None

6. Bibliography

   System Administration 4.1.2 Student Guide, Sun Microsystems

4.2.2.2 Adding a Dataless Client to a Server

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

   Dataless clients should be added as needed.

2. Preconditions

   This is a complex operation and should be done in the presence of an experienced Unix administrator.

3. Goal

   To install a fully functional workstation that contains " /" and "/swap" on a local disk and relies on the file server for "/usr" as well as other file systems.

4. Operating Instructions

   A. Operating Instructions

   B. Run "suninstall" as per the Sun installation manual instructions.

   C. Provide a machine name as assigned by the System Administrator and the next IP address in sequence. You can find the last IP address with the yp command.

      % ypcat hosts

   D. After "suninstall" terminates, reboot the system.

   E. Edit "/etc/hosts" file to include the NIS server.

   F. Modify the NIS server machine's "/etc/hosts" file to include the new machine.

   G. Copy the "/etc/printcap" file from any dataless host (except the print server) to the new machine.

   H. Replace "/etc/rc" and "/etc/rc.local" files with corresponding files from any other dataless host.

I. Modify /etc/fstab file to match other dataless hosts.

J. Reboot the system.

5. Related Policies

None

6. Bibliography

System Administration 4.1.2 Student Guide, Sun Microsystems

4.3 UNIX ADMINISTRATION

4.3.1 Message Of The Day Administration

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

The "Message Of The Day" is to convey information to system users. Examples of information displayed in the message of the day can be the phone number and e-mail address for the hotline or dates and reasons the system may be down. The "Message Of The Day" changes when all users require new information or when information in the current "Message Of The Day" is no longer correct.

2. Preconditions

Superuser privileges and access to the master NIS server are required.

3. Goal

The goal is to supply all users with new or updated information.

4. Operating Instructions

A. Become superuser on the NIS server.

B. Edit the "/etc/motd" file to reflect whatever information you want contained in the "Message Of The Day".

C. Copy the Server's "/etc/motd" to all machines on the LAN.".

5. Related Policies

None

6. Bibliography

System Administration 4.1.2 Student Guide, Sun Microsystems

4.3.2 Mail Alias Administration

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

The mail aliases file allows users to send mail to a group of users referenced by a single name The mail aliases are updated when users are added to or deleted from the system. or. for many possible reasons, a user requires membership in an alias.

2. Preconditions

Superuser privileges and access to the master NIS server are required.

3. Goal

The goal is to supply users with the ability to send mail to necessary users referenced by a single name.

4. Operating Instructions

A. As superuser on the NIS server, edit the "/etc/aliases" file.

B. Make whatever changes are needed in the file, then save it.

C. Change directory to "/var/yp" and enter the following command;

% make

5. Related Policies

None

6. Bibliography

System Administration 4.1.2 Student Guide, Sun Microsystems

4.3.3 System Administration Logging

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

   The System Administration Log is necessary to track all changes made to the system and all actions taken to correct a problem with the system. The log shall be updated when changes are made and actions are taken.

2. Preconditions

   A change will have been made to the system.

3. Goal

   The goal is to track all changes made to the system for future reference and disaster recovery.

4. Operating Instructions

   A. Make a note of significant changes that were made to the system Each entry in the log shall include the date and the machines affected, description of actions taken, and the reasoning for the actions taken.

5. Related Policies

   None

4.3.4 Manual Page Administration

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

   Manual pages (man pages) are updated when a new product is added to the system, or when a product is updated on the system.

2. Preconditions

   A product is added to the system, or is updated on the system. Man pages are normally supplied with a product.

3. Goal

   The goal is to supply users with current information on products or the system.

4. Operating Instructions

A. Sign on to the system as "root".

B. The directories "/usr/share/man/man?" correspond to each chapter of the manual. New man pages are placed in the directory mann. Copy the new man pages into their chapter. Each man page must end with an extension of "<chapter>". For example, a new man page for "foo" in mann would have the name "foo.n".

C. Make the new man page(s) visible to the whatis(1) command by using the command;

```
% /usr/lib/makewhatis
```

D. Log appropriate information in the System Administrators log book.

5. Related Policies

None

6. Bibliography

System Administration 4.1.2 Student Guide, Sun Microsystems

4.3.5 Premeditated System Shutdown

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

The shutdown is performed as needed, usually for system maintenance.

2. Preconditions

A premeditated system shutdown is performed after users are notified. The "Message Of The Day" will be used to notify users of premeditated system shutdowns.

3. Goal

The goal is to shutdown the system to allow for maintenance.

4. Operating Instructions

A. Inform the users of the shutdown, via "Message Of The Day", with a mini mum of one week in advance, if possible. In the "Message Of The Day", give the time and date of the shutdown and the reason for the shutdown.

B. Sign on to the system being shutdown as "root".

C. Stop the multi-user and networking capabilities of the system by issuing the command;

% shutdown now

D. If you desire to halt the operating system and go to the EPPROM prompt, issue the command;

% halt

E. If you desire to turn the power off for the system, power off the monitor, then the CPU, and then additional external devices, if attached.

5. Related Policies

None

6. Bibliography

System Administration 4.1.2 Student Guide, Sun Microsystems

4.3.6 Emergency System Shutdown

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

An emergency system shutdown occurs when for some unexpected reason the system must be shutdown. An emergency system shutdown is immediate and little, if any, notice is usually given to the users.

2. Preconditions

A situation must occur that requires the system to be shutdown immediately.

3. Goal

The goal is to immediately shutdown the system, while maintaining the integrity of the system.

4. Operating Instructions

A. Inform the users of the shutdown, if possible.

B. Try to login to the machine being shutdown and run the "sync" command. This forces the system to complete any writes to the disk and forces the system to update the superblock.

C. Shutdown and halt the operating system using a keyboard initiated system halt.

D. If you desire to turn the system power off, power off the monitor, then the CPU, and then any additional external devices, if attached.

E. Upon making the system operational, send a "Message of The Day" explaining the problem.

5. Related Policies

   None

6. Bibliography

   System Administration 4.1.2 Student Guide, Sun Microsystems

4.4 AFS ADMINISTRATION

The procedures described in this section are specific to AFS. More detail on the commands that are described can be found in the AFS System Administrator's Guide if needed.

4.4.1 Installing Additional Client Machine(s)

Responsible Role: System Administrator

Supporting Role: N/A

The process for adding additional AFS client machines is described in detail in the AFS System Administrator's Guide.

4.4.2 Adding User Accounts

Responsible Role: System Administrator

Supporting Role: User Support

1. Frequency

   User accounts will be added as needed.

2. Preconditions

The System Administrator must receive approval to add the account via an authorization form from User Support.

3. Goal

The goal is to set up an AFS account that will allow the owner of the account to access the resources that they are authorized to access via AFS.

4. Operating Instructions

A. Pre-select the following:

A user name. If the user has an Unix account, use the Unix user account name. If the user does not have a Unix user account, then a name must be chosen by the System Administrator.

An AFS UID. If the user has an Unix account, use the Unix UID. If the user does not have a Unix user account, then a UID must be chosen by the System Administrator.

An initial dummy password. Advise the user to change this at first logon.

B. Verify you have the privileges necessary to add an account:

You belong to system:administrators.

You are included in /usr/afs/etc/UserList.

You have the ADMIN flag in your Authentication Database entry.

You are logged on the file server.

You are klogged as root on the file server.

You know the "root" password for the file server.

C. Create the account:

Add the user to the AFS Protection and Authentication Database using AFS's User Services:

% uss add -user "<Username>" -uid "$<UID>" -pass "<AFS Password>"

5. Related Policies

None

6. Bibliography

AFS System Administrator's Guide

4.4.3 Delete a User Account

Responsible Role: System Administrator

Supporting Role: User Support

1. Frequency

   User accounts will be deleted as needed.

2. Preconditions

   The System Administrator must receive approval to delete the account via an authorization form from User Support.

3. Goal

   The goal is to completely remove a user's AFS account, denying them access to resources.

4. Operating Instructions

   A. Verify that you have the privileges necessary for performing the following steps:

      You belong to system:administrators.

      You are included in /usr/afs/etc/UserList.

      You are logged on the file server.

      You are klogged as root on the file server.

      You know the "root" password for the file server.

   B. Delete the account:

      Remove the user from the AFS Protection Database:

      % pts delete <Username>

      Remove the user from the AFS Authentication Database:

      % kas delete <Username>

5. Related Policies

   None

6. Bibliography

   AFS System Administrator's Guide

4.4.4 Creating a Group

Responsible Role: CARDS Users

Supporting Role: System Administrator

1. Frequency

   Groups will be created as needed.

2. Preconditions

   A user with an AFS account may create groups as needed. Users shall also maintain groups that they create.

3. Goal

   The goal is to aid in file sharing among AFS users, and to control access to resources.

4. Operating Instructions

   A. There are a few constraints on the form of group names and who may own groups. Violation of the constraints results in an error message and failure to create the group. The group-name field may include any lowercase letters, numbers and punctuation except the colon and the period. Names can be up to 63 characters long. Short group-names are preferable because they must always be typed in full, but they should also give some indication of the nature of the group. Use meaningful names - it is difficult to remember which group is which if they all have names like terry:1, terry:2 and so on.

   B. Verify that you have the privilege necessary for creating groups or setting up AFS UIDs (membership in system:administrators). If necessary, issue pts membership on your own entry; you always have the right to do this. If you are not a member of system:administrators, the name of your group must be in the form of <Your username>:<Group name>.

      % pts creategroup -name <group name> —owner [<owner of the group>] -id [<ID for the group>]

5. Related Policies

   None

6. Bibliography

   AFS System Administrator's Guide

4.4.5 Deleting a Group

Responsible Role: CARDS Users

Supporting Role: System Administrator

1. Frequency

   Groups will be deleted as needed.

2. Preconditions

   The System Administrator must receive approval to delete a group via an authorization form from User Support.

   A user with an AFS account may delete groups that they own as needed.

3. Goal

   The goal is to completely remove a group from AFS, denying access to resources. Groups may also become obsolete; in this case, groups will be removed to keep the system tidy.

4. Operating Instructions

   A. Verify you have the privilege necessary for removing an entry from the Protection Database. If necessary issue the pts membership on your own entry:

      % pts membership <user name>

   B. Delete each group entry from the Protection Database:

      %pts delete [-name <group name>+] [id <group ID>+]

5. Related Policies

   None

6. Bibliography

   AFS System Administrator's Guide

4.4.6 Add Users to Groups

Responsible Role: CARDS Users

Supporting Role: System Administrator

1. Frequency

Users will be added to groups as needed.

2. Preconditions

   The System Administrator must receive approval to add a user to a group from the owner of the group or via an authorization form from User Support.

3. Goal

   The goal is to allow users to participate in group sharing of files.

4. Operating Instructions

   A. Verify you are entitled to add members to each group. The fourth ("a") privacy flag associated with the entry determines who may add members. If necessary, examine the flags with the pts examine command:

      % pts examine <Groupname>

      The owner of the entry (also visible with pts examine) and members of system:administrators always have the necessary privilege.

   B. Add member(s) to group(s):

      % pts adduser -user <user name>+ —group <group name>+

5. Related Policies

   None

6. Bibliography

   AFS System Administrator's Guide

4.4.7 Delete Users From Groups

Responsible Role: CARDS Users

Supporting Role: System Administrator

1. Frequency

   Users will be deleted from groups as needed.

2. Preconditions

   The System Administrator must receive approval to delete a user from a group from the owner of the group or via an authorization form from User Support.

3. Goal

   To deny user access to selected resources.

4. Operating Instructions

   A. Verify that you are entitled to remove members from each group. The fifth ("r") privacy flag associated with the entry determines who may remove members. If necessary, examine the verify flags with the pts examine command:

      % pts examine <Groupname>

      The owner of the entry (also visible with pts examine) and members of system:administrators always have the necessary privilege.

   B. Remove member(s) from the group(s):

      % pts removeuser -user <user name> —group <group name>

5. Related Policies

   None

6. Bibliography

   AFS System Administrator's Guide

4.4.8 Maintain the Access Control Lists (ACLs)

Responsible Role: CARDS Users

Supporting Role: Configuration Management (CM), System Administrator

1. Frequency

   ACL's will be maintained as needed.

2. Preconditions

   ACL's will only be changed on library directories by CM.

3. Goal

   The goal of changing an ACL is to control access to resources.

4. Operating Instructions

   A. Changing the ACLs

You must have the administrator right on the ACL to change it. Members of system:administators have implicit administer rights on the ACL of every directory. The owner of a directory also has the implicit administer right.

The following shows the syntax for the fs setacl command:

%fs setacl -dir <directory>+ -acl <access list entries>+ [-negative] [-clear]

5. Related Policies

   None

6. Bibliography

   AFS System Administrator's Guide

4.4.9 Volume Maintenance

4.4.9.1 Creating a Volume

Responsible Role: System Administrator

Supporting Role: Configuration Management (CM), CARDS Users

1. Frequency

   Volumes will be created as needed.

2. Preconditions

   The System Administrator must receive a request to create a volume.

3. Goal

   The goal is to create a volume in AFS to store resources.

4. Operating Instructions

   A. Verify you have the privilege necessary for creating volumes. If necessary, issue bos listusers:

      % bos listusers <machine name>

   B. Verify you have the administer and insert rights for the directory in which you wish to mount the volume. If necessary, issue the fs listacl command:

      % fs listacl <directory>

      If you are a member of system:administrators, you have the administrator right on every ACL and can use fs setacl to grant yourself the insert right if necessary.

C. Pre-select a site (disk partition on a file server machine) for the new volume. You may wish to put the volume on the emptiest partition. You can determine how much space is available on a file server machine's partitions (and their total size) with vos partinfo:

% vos partinfo <machine name> [<partition>]

Note: The total partition size reported in this command may not agree with the same figure in the output of the standard UNIX df command. The df total size includes some reserved space that does not show up in this report and so is likely to be about 10% larger.

D. Pre-select a name (22 characters or less) for the volume. The Volume Server will not allow you to create a volume with a longer name.

E. Create the volume:

% vos create <machine name> <partition name> <volume name>

F. Mount the new volume in the file tree so that its contents are visible:

% fs mkmount <directory> <volume name> [-rw]

-rw should be included only in the rare cases where you want the mount point to be a ReadWrite one.

G. Verify you have created the mount point correctly with the fs lsmount command.:

% fs lsmount <directory>

5. Related Policies

None

6. Bibliography

AFS System Administrator's Guide

4.4.9.2 Deleting a Volume

Responsible Role: System Administrator

Supporting Role: Configuration Management (CM), CARDS Users

1. Frequency

Volumes will be deleted as needed.

2. Preconditions

The System Administrator must receive a request to delete a volume from someone authorized by CM to make such a request or by the owner of the volume.

3. Goal

   The goal is to remove any unwanted volumes in an effort to conserve computer resourc es and keep the system tidy.

4. Operating Instructions

   A. Verify you have the privilege necessary for removing volumes (inclusion in /usr/afs/etc/UserList). If necessary, issue bos listusers:

      % bos listusers <machine name>

   B. Verify you have the delete right for the directory from which you wish to remove the volumes's mount point. If necessary, issue the fs listacl command:

      % fs listacl <directory>

      If you are a member of system:administrators, you have the administrator right on every ACL and can use fs setacl to grant yourself the delete right if necessary.

   C. Dump the volume in preparation for saving it permanently on tape. This step is advisable, since you may want to restore the volume later.

      % vos dump <volume name or ID> 0 <dump file>

   D. Remove the volume:

      % vos remove <machine name> <partition name> <volume name or ID>

   E. Remove the mount point, but not if any copies of the Read Only version will remain on the file system and you wish them to be accessible.

      % fs rmmount <directory>

   F. If you created a dump file in step C, transfer it to tape. The preferred method is to use the AFS Backup System.

5. Related Policies

   None

6. Bibliography

   AFS System Administrator's Guide

4.4.9.3 Moving a Volume

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

   Volumes will be moved as needed.

2. Preconditions

   Volumes may be moved as part of an effort to reorganize. However, volumes will usually be moved when the partition they are stored on becomes full.

3. Goal

   The goal of moving a volume to a new partition is to create more space for volumes to grow within a partition.

4. Operating Instructions

   A. Verify you have the privilege necessary for moving volumes (inclusion in / usr/afs/ect/UserList). If necessary, issue bos listusers.

      % bos listusers <machine name>

   B. Move the volume. Type the following command on a single line:

      vos move <volume name or ID> <machine name on source> <partition name on source> <machine name on destination> <partition name on destination>

   C. Confirm the move was successful using the vos listvldb command.

      % vos listvldb <volume name or ID>

   D. If a Backup version of the volume existed at the ReadWrite's previous site, create a new Backup at the new site:

      % vos backup <volume name or ID>

5. Related Policies

   None

6. Bibliography

   AFS System Administrator's Guide

4.4.9.4 Setting Volume Quota

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

   Setting volume quotas will be done as needed.

2. Preconditions

   Volume quotas will be set when new volumes are created. Volume quotas may also be reset when more storage is required within a volume or when volume growth must be restricted.

3. Goal

   The goal of resetting a volume quota is to allow for further growth or restrict further growth within the volume.

4. Operating Instructions

   A. Verify you have the privilege necessary to set the volume quota (membership in the system:administrators group). If necessary, issue the pts membership command:

      % pts membership system:administrators

   B. Set maximum quota on one or more volumes:

      % fs setvol <directory>+ -max <disk space quota in 1K units>

5. Related Policies

   None

6. Bibliography

   AFS System Administrator's Guide

4.4.9.5 Monitor Volume Usage

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

   Volume usage will be monitored once a week or as needed.

2. Preconditions

   If a partition becomes too full, volumes will need to be moved. Monitoring volume usage will be required to determine which volumes to move and where.

3. Goal

   Volumes will be monitored to ensure all users have adequate work space.

4. Operating Instructions

   A. At the command shell prompt (%), type:

      % fs quota <directory>+

5. Related Policies

   None

6. Bibliography

   AFS System Administrator's Guide

4.4.10 The Backup System

4.4.10.1 Label Tapes

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

   Tapes will be labeled or relabeled as needed.

2. Preconditions

   Tapes will be labeled automatically if there are no AFS labels currently on the tapes. Tapes will also be relabeled if a tape is being reused and the current label is incorrect.

3. Goal

   The goal of labeling tapes is to help prevent accidental loss of data.

4. Operating Instructions

   It is not essential to pre-label tapes because the backup system can use unlabeled or partially labeled tapes. The Backup System checks each tape before writing to

it; if the tape is labeled incorrectly, the dump cannot proceed until you insert an acceptable tape in the drive. It may be necessary to label the tape correctly if it is incorrectly labeled. It is a good idea to read the current tape label before you relabel a tape, just to make certain you want to relabel it. To read a tape label use the following procedure:

A. Open two command windows.

B. In one window start the backup tape controller by typing:

% butc 0

C. In the other window, read the tape label by typing:

% backup readlabel

To relabel a tape with name and size use the following procedure:

A. Place the tape to be read into the tape drive.

B. Enter openwindows on the AFS backup server by typing:

% openwin - noauth

C. In one window start the backup tape controller by typing:

% butc 0

D. In the other window label the tape by typing:

% backup labeltape <tape name> <tape size>

5. Related Policies

None

6. Bibliography

AFS System Administrator's Guide

4.4.10.2 Perform Backups

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

Backups will be performed daily.

2. Preconditions

   The System Administrator must be logged in and klogged in as admin.

3. Goal

   The goal of performing backups is to preserve the integrity of the library.

4. Operating Instructions

   It is assumed that the backup volume set and backup dump hierarchies have already been defined. If this is not true then refer to the AFS System Administration Manual dumps are to be done during normal working hours.

   A. Open two command windows.

   B. In one window start the backup tape controller by typing:

      % butc 0

   C. In the other window enter backup interactive mode by typing:

      % backup

      The "<backup>" prompt will appear in the window.

   D. To list the dump hierarchies type the following, while in backup interactive mode window:

      backup> listdump

   E. To start the backup type at the backup prompt:

      backup> dump <volume set name> <dump level name>

5. Related Policies

   None.

6. Bibliography

   AFS System Administrator's Guide

4.4.10.3 Restore Procedures

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

Volumes will be restored as needed.

2. Preconditions

   A user will request that a volume be restored.

   Make certain you are kloged as admin (where admin is an actual user). You must also be logged in to the Unix system as admin. You may need to use the su command to login properly.

3. Goal

   The goal of restoring a volume is to restore volumes to a previous state.

4. Operating Instructions

   A. Enter openwindows on the AFS backup server by typing:

      % openwin -noauth

   B. Open two command windows.

   C. In one window start the backup tape controller by typing:

      % butc 0

   D. In the other window enter the backup interactive mode by typing:

      % backup

      The 'backup>' prompt will appear in the window.

   E. Place the proper backup tape into the tape drive. You can use the backup scantape command to extract dump set information from a tape while in backup interactive mode window by typing:

      backup> scantape

   F. Issue the volrestore command with the desired arguments, using the following examples as a guide:

      backup> volrestore <destination machine> <destination partition> <volumes to restore> -extension <new volume extension> -date <restore date to use>

5. Related Policies

   None

6. Bibliography

AFS System Administrator's Guide

4.4.11 System Password Administration

Responsible Role: System Administrator

Supporting Role: N/A

1. Frequency

   The password should be changed on a periodic basis with the period not to exceed four months in length.

2. Preconditions

   The AFS Administrator password is to be known only by the System Administrator.

3. Goal

   The goal of changing the AFS Administration password is to maintain system security.

4. Operating Instructions

   Changing the system password is performed using the following command:

   % kpasswd

5. Related Policies

   None

6. Bibliography

   AFS System Administrator's Guide

4.5 SYBASE ADMINISTRATION

The procedures described in this section are specific to the Sybase database system. More detail on the described commands can be found in the Sybase System Administration Guide if needed. In this section the terms Database Administrator and System Administrator are used interchangeably; "Authorization/workorder" refers to Hotline User Request/Hotline Staff Workorder.

4.5.1 Add Login Names

Responsible Role: Database Administrator

Supporting Role: N/A

1. Frequency

   As needed.

2. Preconditions

   Before adding a login name to the SQL server, the Database Administrator must have the appropriate authorization/work order specifying the login name to be added.

3. Goal

   To provide users with sybase accounts as requested.

4. Operating Instructions

   The process of adding a new login name is performed using the following command:

   % sp_addlogin <loginame> [,password [,defaultdb]

   The System Administrator creates a login account for the user with the sp_addlogin command. This command can only be performed by the System Administrator.

   The first parameter, loginame, is required and must be unique on the SQL server following the rules for identifiers.

   The second parameter is a password for the new user. If no password parameter is given, the default NULL password is given.

   The third parameter, defaultdb, specifies the user database to which the user is given access when the connection to the SQL server is established. If no default database is specified, the user is assigned to the master database.

5. Related Policies

   None

6. Bibliography

   Sybase Administration Guide

4.5.2 Drop Login Names

Responsible Role: Database Administrator

Supporting Role: N/A

1. Frequency

   As needed.

2. Preconditions

   Before dropping a login name from the SQL server, the System Administrator must have the appropriate authorization/work order specifying the login name to be dropped.

3. Goal

   To delete database accounts as requested or to deny unauthorized user access to the server.

4. Operating Instructions

The command sp_droplogin denies a user access to the SQL server.

The process of dropping a login name is performed using the following command:

% sp_droplogin <loginname>

5. Related Policies

   None

6. Bibliography

   Sybase Administration Guide

4.5.3 Add User

Responsible Role: Database Administrator

Supporting Role: Database Owner

1. Frequency

   As needed.

2. Preconditions

   Before adding a user to a database, the System Administrator or the Database Owner must have the appropriate authorization/work order specifying the user to be added and to which database(s) the user needs to be added to.

3. Goal

To give database users access to specific databases as requested.

4. Operating Instructions

The command sp_adduser adds a user to a specified database. The System Administrator must have already added the user to the SQL server with sp_addlogin.

The process of adding a user to a database is performed using the following command:

% sp_adduser <loginame> [,name_in_db [,group_name]]

The first parameter to sp_adduser is the login name of an existing user and it is a required parameter. The second and third parameters are optional.

The second parameter, name_in_db, allows the Database Owner to specify a name different from the login name by which the user is to be known inside the database. If no name_in_db is specified, the name inside the database is the same as the login name.

The third parameter, group_name, also optional, is the name of an existing group in the database. If no group name is specified, the user is made a member of the default group public.

5. Related Policies

None

6. Bibliography

Sybase Administration Guide

4.5.4 Drop User

Responsible Role: Database Administrator

Supporting Role: Database Owner

1. Frequency

As needed.

2. Preconditions

Before dropping a user from a database, the System Administrator or the Database Owner must have the appropriate authorization/work order specifying the user to be dropped and from which database(s) the user needs to be dropped from.

3. Goal

To deny specific users access to specific databases as requested.

4. Operating Instructions

The command sp_dropuser denies a SQL server user access to the database in which it is executed.

The process of dropping a user from a database is performed using the following command:

% sp_dropuser <r.me_in_db>

5. Related Policies

None

6. Bibliography

Sybase Administration Guide

4.5.5 Sybase Password Administration

Responsible Role: Database Administrator

Supporting Role: N/A

1. Frequency

Periodic intervals not exceeding four months in length.

2. Preconditions

The Database Administrator becomes aware of conditions suggesting that the change of a password is in order, or four months after the last change of the Sybase system administration password or the Sybase account password.

The Sybase System Administrator password as well as the UNIX Sybase account pass word are only to be known by the Sybase System Administrator and the Sybase Backup System Administrator.

3. Goal

To protect the system from unauthorized access and to restrict the knowledge of system administration passwords to the Sybase System Administrator and the Sybase Backup System Administrator.

4. Operating Instructions

Sybase user passwords should be changed on a regular basis and can be changed by the System Administrator without notice if there is any evidence of system misuse.

A user can change his/her password at any time with the command sp_password. The System Administrator can use this command to change his/her own password or any other user's password.

The sp_password command syntax follows:

% sp_password <old>,<new> [, login name]

The first two parameters are required, whether the command is being executed by the System Administrator or another user. Only the System Administrator has permission to use the third parameter to change other user's passwords.

Passwords that include characters other than A-Z, a-z, and 0-9 must be typed in quotation marks.

5. Related Policies

   None

6. Bibliography

   Sybase Administration Guide

4.5.6 Add Group

Responsible Role: Database Administrator

Supporting Role: Database Owner

1. Frequency

   As needed.

2. Preconditions

   Before creating a group, the System Administrator or the Database Owner must have the appropriate authorization/work order specifying the group to be created, the data base where the group needs to be created, and the users to be included in the group if any.

3. Goal

   To provide groups of users access privileges to a specific database as requested.

4. Operating Instructions

Groups provide a collective name for granting and revoking privileges. The command sp_addgroup can be executed by the Database Owner or the System Administrator in the database to which the group is to be added.

The process of adding a group is performed using the following command:

% sp_addgroup <group_name>

5. Related Policies

None

6. Bibliography

Sybase Administration Guide

4.5.7 Change Group

Responsible Role: Database Administrator

Supporting Role: Backup Database Administrator, Database Owner

1. Frequency

As needed.

2. Preconditions

Before changing a group, the System Administrator or the Database Owner must have the appropriate authorization/work order specifying the group to be changed, the data base in which it needs to be changed, and the user(s) to be added to the group or dropped from the group.

3. Goal

To modify the membership of a group as requested.

4. Operating Instructions

Changegroup is used to modify an existing group's affiliation. At any one time, each user can be a member of only one group.

The process of changing a group's membership is performed using the following commands:

A. To change a user from his/her current group to another group use the following format:

% sp_changegroup <group_name>, <name_in_db>

B. To remove a user from a group without assigning the user to another group, change the affiliation to "public". The name "public" must be in quotes because it is a reserved word. The command is as follows:

% sp_changegroup <"public">, <name_in_db>

5. Related Policies

None

6. Bibliography

Sybase Administration Guide

4.5.8 Drop Group

Responsible Role: Database Administrator

Supporting Role: Database Owner

1. Frequency

As needed.

2. Preconditions

Before dropping a group, the System Administrator or the Database Owner must have the appropriate authorization/work order specifying the group to be dropped and the database from which the group needs to be dropped from.

3. Goal

To delete groups no longer needed as requested.

4. Operating Instructions

A group that has members cannot be dropped. An error message displays a list of the members of the group that you are trying to drop. To remove users from a group execute sp_changegroup.

The process of dropping a group is performed using the following command:

% sp_dropgroup <group_name>

5. Related Policies

4.5.7 Change Group

6. Bibliography

Sybase Administration Guide

4.5.9 Changing the Default Database

Responsible Role: Database User

Supporting Role: Database Administrator

1. Frequency

   A user can change his/her default database at any time.

2. Preconditions

   The System Administrator, prior to changing any user's default database, must notify the user of the change.

3. Goal

   To control which users access specific databases.

4. Operating Instructions

The command sp_defaultdb does not automatically give the user access to the database specified. Unless the Database Owner has set up access with sp_adduser or sp_add alias, the user is connected to master even after his/her default database has been changed.

The process of changing a user's default database is performed using the following command:

% sp_defaultdb <loginame>, <defaults>

5. Related Policies

   None

6. Bibliography

   Sybase Administration Guide

4.5.10 Creating Alias Users

Responsible Role: Database Owner

Supporting Role: Database Administrato·

1. Frequency

As needed.

2. Preconditions

Database Owners are able to create database aliases at their discretion. Users that will be affected by the alias should be notified by the Database Owner.

3. Goal

To provide the Database Owner with a way to treat multiple database users as a single user allowing the Database Owner to apply one action to multiple users at one time.

4. Operating Instructions

The sp_addalias command allows the dbo (Database Owner) to treat more than one person as the same user inside a database, giving all of them the same privileges. The alias mechanism is often used to give the role of dbo to several users.

The process of creating an alias is performed using the command sp_addalias as follows:

% sp_addalias <loginame>, <name_in_db>

The first parameter, loginame, is the name of the user who is being assigned an alternate identity in the current database. The user must have an account on the SQL server.

The second parameter is the name of the database user to whom the first user wishes to be linked. Both parameters are required.

The sp_addalias command must be performed in the database in which the alias is wanted.

5. Related Policies

None

6. Bibliography

Sybase Administration Guide

4.5.11 Dropping Aliases

Responsible Role: Database Owner

Supporting Role: Database Administrator

1. Frequency

   As needed.

2. Preconditions

   Users that will be affected should be notified by the Database Owner.

3. Goal

   To delete aliases no longer needed.

4. Operating Instructions

The sp_dropalias command is used to drop a user's alias. Once the alias is dropped, the user no longer has access to the database unless he/she is also a user of the database or has another alias in that database.

The process of dropping an alias is performed using the following command:

% sp_dropalias <loginame>

5. Related Policies

   None

6. Bibliography

   Sybase Administration Guide

4.5.12 Maintaining Permission Hierarchies

Responsible Role: Database Administrator

Supporting Role: N/A

1. Frequency

   N/A

2. Preconditions

   In the four level Sybase permission hierarchy, each of the three lower levels (Database Owners, Database Object Owners, and public) has its own discretion in assigning permissions to a given user. The top level, the System Administrator, can perform some commands that no other user can. Access to this level must be restricted to the System Administrator and a Backup System Administrator only. This is enforced by maintaining a System Administrator's password that only these two people know.

3. Goal

To limit database user's permissions only to the permissions that each user needs.

4. Operating Instructions

At each level of the hierarchy, different permissions are automatically assigned and different ones can be granted.

The Sybase System Administrator is recognized by the SQL server as a superuser who works outside of the SQL server's protection system.

Database Owners are next in the hierarchy. Database Owners and the System Administrator are the only users who can grant command permissions to other users.

At the next level are the owners of database objects such as tables, views, and stored procedures, who control permissions on those objects; no other users have permission on those objects until the owner specifically grants to them with the GRANT command.

At the bottom of the hierarchy is the "public" (other database users). Permissions are granted to or revoked from the public by Object Owners, Database Owners, and/or the System Administrator.

For a list of permission for each level of the hierarchy, see the Sybase Administration Guide.

5. Related Policies

None

6. Bibliography

Sybase Administration Guide

4.5.12.1 Granting and Revoking Permissions

Responsible Role: Database Administrator, Database Owner

Supporting Role: N/A

1. Frequency

As needed.

2. Preconditions

None

3. Goal

To limit database users permissions only to the permissions that each user needs.

4. Operating Instructions

Command permissions and object permissions are assigned or removed with the GRANT and REVOKE commands.

The syntax for command permission is slightly different from the syntax for object permissions. The GRANT and REVOKE command syntax statements follow:

%GRANT {ALL | <command_list>+}
TO {PUBLIC | <name_list>+}

%REVOKE {ALL | <command_list>+}
FROM {PUBLIC | <name_list>+}

The command list can include the following commands:

CREATE DATABASE (can be granted only by the System Administrator), CREATE DEFAULT, CREATE PROCedure, CREATE RULE, CREATE TABLE, CREATE VIEW, DUMP DATABASE, and DUMP TRANsaction.

Only the System Administrator can use the keyword ALL when granting command permissions.

The syntax for granting and revoking object permissions (permissions on tables, views, columns, and stored procedures) follow:

% GRANT {ALL | <permission_list>+}
ON {<table_name> [<column_list>+] |
view_name [<column_list>+] |
<stored_procedure_name>}
TO {PUBLIC | <name_list>+}

%REVOKE {ALL | <permission_list>+}
ON {table_name> [<column_list>+] |
<view_name> [<column_list>+] |
<stored_procedure_name>}
FROM {PUBLIC | <name_list>+}

When you grant or revoke permissions on a table or view, without specifying any columns, the privilege list can consist of any combination of SELECT, INSERT, DELETE, and UPDATE.

When you grant or revoke permissions on columns, the privilege list can include only SELECT and UPDATE. If a user needs to be able to use a SELECT statement, he/she must be granted SELECT permission on the table, or on all the columns in the table.

When you grant or revoke permissions on stored procedures, the privilege list can only consist of EXECute or ALL, which is understood as a synonym for EXECute.

The C clause in a GRANT or REVOKE statement specifies the object on which the permission is being granted or revoked. You can grant or revoke permissions for only one table, view, or stored procedure at a time. You can grant or revoke permissions to more than one column at a time, but all the columns must be on the same table or view.

The keyword PUBLIC refers to all the users of the SQL server.

5. Related Policies

   None

6. Bibliography

   Sybase Administration Guide

4.5.13 Managing Physical Resources

4.5.13.1 Initialization of Database Devices

Responsible Role: Database Administrator

Supporting Role: N/A

1. Frequency

   As needed.

2. Preconditions

   Prior to allocating space for database storage, the System Administrator must have the appropriate authorization/work order specifying the required size for the space to be allocated.

3. Goal

   To define and prepare system storage devices to be used for database storage.

4. Operating Instructions

A database device (disk partition or file) is dedicated to the storage of the objects making up databases. Each database device must be prepared and made known to the SQL server before it can be used to store a database.

An initialized database device can be:

Allocated to the pool of space available to a user database.
Allocated to a user database and assigned to store specific database
Designed as a default device for CREATE and ALTER DATABASE commands.

The database administrator uses the DISK INIT command to create new database devices. The syntax for the DISK INIT command follows:

NAME = <"device_name">,
PHYSNAME = <"physical name">,
VDEVNO = <"virtual device number">,
SIZE = <"number of 2K blocks">

The NAME is the name of the database device (a valid identifier).

The PHYSNAME, or the physical name of the device, is the name of the raw disk partition in Unix.

The VDEVNO, or virtual device number, is an identifying number for the database device. It is a number between 1-255 but it cannot be greater than the number of database devices for which the system is configured. This number must be unique among devices used by the SQL server.

The SIZE of the database device is given in 2K blocks. There are 512 - 2K blocks in a megabyte. If a new device is going to be used for the creation of a new database, the minimum SIZE is the size of model, 1024 - 2K blocks (2 megabytes).

To successfully complete disk initialization, the Sybase System Administrator executing the DISK INIT command must have the appropriate operating system permissions on the device that is being initialized.

5. Related Policies

   None

6. Bibliography

   Sybase Administration Guide

4.5.13.1.1 Designating Default Devices

Responsible Role: Database Administrator

Supporting Role: N/A

1. Frequency

   As needed.

2. Preconditions

   The database device must already exist.

3. Goal

To control the location of user databases.

4. Operating Instructions

If a pool of default database devices is wanted that will be used by all SQL server users for creating databases, use the sp_diskdefault command after the devices have been initialized with DISK INIT.

The syntax for sp_diskdefault follows:

% sp_diskdefault <device_name>, {defaulton | defaultoff}

Users can have multiple default devices. They are used in the order in which they appear in the system table sysdevices.

5. Related Policies

None

6. Bibliography

Sybase Administration Guide

4.5.13.2 Creating Databases

Responsible Role: Database Administrator

Supporting Role: N/A

1. Frequency

As needed.

2. Preconditions

Prior to creating a database, the System Administrator must have the appropriate authorization/work order specifying the required size and the name of the database to be created.

3. Goal

To create user databases as requested.

4. Operating Instructions

The CREATE DATABASE command can be issued only by the System Administrator while using the master database.

The syntax for the CREATE DATABASE command follows:

% CREATE DATABASE <database_name>
[ON {DEFAULT | <database_device>} [= <size>]
[, <database_device> [= <size>]]+]
[LOG ON <database_device> [= <size>]] [, <database_device> [<size>]]+]
[FOR LOAD]

A database name must follow the rules for identifiers. Only one database can be created at a time.

The option ON clause allows you to specify the name(s) of one or more database devices and the allocation of each database device in megabytes.

If the keyword DEFAULT is used, or if the ON clause is omitted, the database is stored on one or more of the default database devices.

The optional LOG ON clause places the transaction log on a separate database device and limits it to the specified size which keeps it from competing with other database activity for space. The LOG ON clause also allows you to use the DUMP TRANsaction command (rather than DUMP DATABASE), resulting in savings in time and tapes. If the LOG ON clause is omitted, the database's transaction log is placed on the same database device as the data tables.

5. Related Policies

   None

6. Bibliography

   Sybase Administration Guide

4.5.13.3 Dropping Databases

Responsible Role: Database Administrator

Supporting Role: N/A

1. Frequency

   As needed.

2. Preconditions

   Prior to dropping a database, the System Administrator must have the appropriate authorization/work order specifying the name of the database to be dropped.

3. Goal

   To remove databases no longer needed.

4. Operating Instructions

Removing a database is accomplished with the DROP DATABASE command which deletes the database and all its objects from the SQL server, frees the storage space that had been allocated for it, and deletes references to the database in the master database.

The syntax for the DROP DATABASE command follows:

% DROP DATABASE<database_name> [, <database_name>]+

After a database has been dropped, a dump of the master database should be performed to ensure recovery in case the master database is damaged.

5. Related Policies

None

6. Bibliography

Sybase Administration Guide

4.5.13.4 Changing Database Ownership

Responsible Role: Database Administrator

Supporting Role: Database Owner

1. Frequency

As needed.

2. Preconditions

Prior to changing database ownership, any users affected must be notified.

3. Goal

To change ownership privileges on a specified database.

4. Operating Instructions

The system procedure sp_changedbowner can be used to change the ownership of a database. This command must be issued in the database whose ownership will be changed.

The syntax for the sp_changedbowner command follows:

% sp_changedbowner <loginame> [, true]

The new owner must already have a login name on the SQL server, but cannot be a user of the database, or have an alias in the database. sp_dropuser or

sp_dropalias may need to be used before the ownership of the database can be changed.

To transfer aliases and their permissions to the new dbo, add the second parameter with the value of TRUE.

5. Related Policies

   None

6. Bibliography

   Sybase Administration Guide

4.5.13.5 Alter Database

Responsible Role: Database Owner

Supporting Role: Database Administrator

1. Frequency

   As needed.

2. Preconditions

   There must be available space in a database device for the database alteration.

3. Goal

   To increase the available space allocated to a database.

4. Operating Instructions

If the space allocated for a database becomes insufficient, it can be increased with the ALTER DATABASE command. Permission for this command defaults to the Database Owner. ALTER DATABASE permission cannot be changed with the GRANT or REVOKE commands.

The syntax for ALTER DATABASE follows:

```
% ALTER DATABASE <database_name>
[ON {DEFAULT | <database_device>] [= <size>]
[, <database_device> [=<size>]]+]
[FOR LOAD]
```

If no size or device is specified, the increase is two megabytes (1024 2K blocks) in the allocated storage space on a default database device.

The ON clause allows for the specification of space on a default database device or on some other database device. The minimum increase that can be specified is one megabyte.

The FOR LOAD option is used only for duplicating space allocation when loading a dump into a new database (see Sybase Administration Guide).

5. Related Policies None

   None

6. Bibliography

   Sybase Administration Guide

4.5.13.5.1 Alter Database and Transaction Logs

Responsible Role: Database Owner

Supporting Role: Database Administrator

1. Frequency

   As needed.

2. Preconditions

   There must be available space in a database device for the database alteration.

3. Goal

   To increase the available space allocated to a database log.

4. Operating Instructions

   If a database's log is on a separate device and more space is needed for the log, use ALTER DATABASE naming the database device where the log is located.

   % ALTER DATABASE <database_name>
   [ON {DEFAULT | <database_device>] [= <size>]

5. Related Policies

   None

6. Bibliography

   Sybase Administration Guide

4.5.13.6 Creating and Using Segments

Responsible Role: Database Owner

Supporting Role: Database Administrator

1. Frequency

   As needed.

2. Preconditions

   Before creating a segment, the physical device must be initialized with the DISK INIT command and the database device must be made available to the database by the ON clause of CREATE DATABASE or ALTER DATABASE.

3. Goal

   To control the storage location of specific database objects.

4. Operating Instructions

Segments are named subsets of the database devices available to a particular SQL server database. Segment names are used in CREATE TABLE and CREATE INDEX commands to place these database objects on specific database devices.

To create a new segment use the sp_addsegment command as follows:

% sp_addsegment <segment_name>, <database_device_name>

5. Related Policies

   None

6. Bibliography

   Sybase Administration Guide

4.5.13.6.1 Creating Database Objects on Segments

Responsible Role: Database Owner

Supporting Role: Database Administrator

1. Frequency

   As needed.

2. Preconditions

   Before creating a database object on a segment, the segment must have been created.

3. Goal

   To store database objects in specific locations.

4. Operating Instructions

After the segment has been defined in the current database, the CREATE TABLE or CREATE INDEX command uses the ON clause to place an object on the segment. The syntax for the CREATE TABLE and CREATE INDEX commands follow:

% CREATE TABLE <table_name> (<column_name> <datatype>)
ON <segment_name>

CREATE [CLUSTERED | NONCLUSTERED] INDEX
<index_name>
ON <table_name> (<column_name>)
ON <segment_name>

Other commands used to modify segments are:

% sp_extendsegment <segment_name>, <device_name>
% sp_placeobject <segment_name>, <object_name>

For more detailed information on segments and their usage see the Sybase User's Guide and Sybase Administration Guide.

5. Related Policies

None

6. Bibliography

Sybase Administration Guide

4.5.14 Database Backups

4.5.14.1 Backup Procedures

Responsible Role: Database Administrator

Supporting Role: N/A

1. Frequency

As specified in the backup schedule.

2. Preconditions

Before performing a database backup (dump), the appropriate dump device must be defined if it does not already exist.

3. Goal

   To provide the ability to reconstruct databases with minimum loss in case of data loss or device failure.

4. Operating Instructions

   A. The use of a tape drive for backups is strongly recommended.

   B. Each database should be dumped immediately after it is created to have a base point, and on a fixed schedule or as needed thereafter.

5. Related Policies

   None

6. Bibliography

   Sybase Administration Guide

4.5.14.2 Backup Schedule

Responsible Role: Database Administrator

Supporting Role: Backup Database Administrator

1. Frequency

   As specified in the following schedule.

2. Preconditions

   None.

3. Goal

   To provide the ability to reconstruct databases with minimum loss in case of data loss or device failure.

4. Operating Instructions

   A. Database transaction logs are dumped daily first thing in the morning during normal working days (see 4.5.14.6 Backing Up Transaction Logs).

   B. Database dumps are made once a week or at the discretion of the Database Owners (see 4.5.14.5 Backing Up Databases).

   C. In addition to dumping each database once a week or as needed, databases must be dumped each time that an operation that is not logged is performed (i.e., bulk

copy, WRITETEXT, and SELECT INTO). It is also recommended to dump a database each time a new index is created.

D. The master database must be dumped after each CREATE DATABASE, ALTER DATABASE, and DISK INIT command is issued.

5. Related Policies

6. Bibliography

Sybase Administration Guide

4.5.14.3 Dump Device Definition

Responsible Role: Database Administrator

Supporting Role: N/A

1. Frequency

As needed.

2. Preconditions

Dump devices accessed with the DUMP and LOAD commands must be located on the machine where the SQL server is running.

3. Goal

To define dump devices with the appropriate parameters.

4. Operating Instructions

The DUMP and LOAD commands use the dump device name in the name column of the sysdevices table and in the device_name column of the report from the sp_helpdevice command.

If the status column contains the values 16 or 24, indicating that the device is a dump device, then the value in the cntrltype column indicates the type of the dump device.

The values in cntrltype for dump devices can be:

2, the dump device can be a disk, part of a disk, a tape drive to be used for single value dumping, or an operating system file. A cntrltype 2 means the dump proceeds without checking for the end of the device.

3-8, indicating a tape dump device. A cntrltype of 3, 4, 5, 6, 7, or 8 means the dump proceeds under the guidance of the console program which prompts the

operator when a new tape is needed. The capacity of the tape dump device is specified with the sp_addumpdevice command.

0, 1, and 9 are not valid values.

Dumping to a file or a disk is not recommended because if there is a disk crash there may be no way to recover the dump. Before dumping to a file, specify its full path using the sp_addumpdevice command and be aware that the contents of the file will be over written.

Tapes are preferred as dump devices since they permit a library of databases and transaction log dumps to be kept off-line. Before issuing a DUMP command, make sure the console program is running and the environment variable DSCONSOLE is defined in the environment (.cshrc or.login file).

Successive dumps to a dump device overwrite the previous dump information on the device.

5. Related Policies

None

6. Bibliography

Sybase Administration Guide

4.5.14.4 Adding and Dropping Dump Devices

Responsible Role: Database Administrator

Supporting Role: N/A

1. Frequency

As needed.

2. Preconditions

Dump devices must be connected to the machine where the SQL server is running.

3. Goal

To add and drop dump devices to and from the system tables.

4. Operating Instructions

A. To add dump devices use the command sp_addumpdevice as follows:

For tape devices:

% sp_addumpdevice "tape", <device_name>, <physical_name>
<physical_name>, <cntrltype>

The cntrltype option is the controller number of the new device. If the dump device being added is a file or disk, the value is 2. If the dump device being added is a tape drive, legal values are 3 through 8.

The parameter skip or noskip is used only if the first parameter is tape. The skip parameter indicates that any tape labels should be ignored when trying to write. The noskip parameter, which is the default, indicates that any existing tape labels should not be ignored.

The size parameter specifies the capacity of tape dump devices used with the console program. For tape dump devices, the tape capacity is specified in megabytes (tape sizes vary depending on the type of tape being used). A tape size must be specified for a tape device since there is no default. The console utility program prompts the operator to change tapes when a data base DUMP reaches the specified capacity of the tape.

B. To drop a dump device use the command sp_dropdevice as follows:

% sp_dropdevice <device_name>

5. Related Policies

None

6. Bibliography

Sybase Administration Guide

4.5.14.5 Backing Up Databases

Responsible Role: Database Owner

Supporting Role: Database Administrator

1. Frequency

Weekly or as needed as specified by the backup schedule.

2. Preconditions

Before dumping a database a dump device must have been specified.

3. Goal

To provide database backups.

4. Operating Instructions

Dumping a database backs up the entire database including the transaction log. The format in which the database is dumped only allows it to be recovered with the LOAD DATABASE command.

The master database, as well as small databases (under 4 megabytes), that store their transaction logs on the same logical device as the rest of the database, should be dumped using the DUMP DATABASE command to backup both the database and the transaction log. A transaction log that is stored on the same device as the rest of the database can also be dumped using the command DUMP TRANsaction WITH TRUNCATE_ONLY.

The syntax of the DUMP DATABASE command follows:

% DUMP DATABASE <database_name>
TO <dump_device>

The database_name is the name of the database that is being dumped. Dump_device is the name of the dump device to which the database that will be dumped.

When the DUMP DATABASE command is issued for a tape dump, the console utility must be running, the DSCONSOLE environment variable must be defined and an operator must be available to respond to the console's prompts.

Permission to dump databases and transaction logs defaults to the Database Owner but generally the Database Administrator performs the dumps.

Larger databases should keep the transaction logs on a different database device than the one(s) containing the rest of the database. This is accomplished using the CREATE DATABASE with the LOG ON extension.

5. Related Policies

   4.5.14.2 Backup Schedule

   4.5.14.6 Backing Up Transaction Logs

6. Bibliography

   Sybase Administration Guide

4.5.14.6 Backing Up Transaction Logs

Responsible Role: Database Owner

Supporting Role: Database Administrator

1. Frequency

   Daily or as specified by the backup schedule.

2. Preconditions

Before dumping a database log, a dump device must have been specified.

3. Goal

To provide database log backups.

4. Operating Instructions

For small databases, the transaction log should not be backed up separately from the database if it is stored on the same device as the rest of the database. This is the case with the master database (its log cannot be stored on a separate device) and may be the case with small user databases (less than four megabytes).

When the log is on a separate device from the rest of the database, it can be backed up with the DUMP TRANsaction command. The backed up copy can be read only with the LOAD TRANsaction command.

The syntax for the DUMP TRANsaction command follows:

% DUMP TRANsaction <database_name>
[TO] <dump_device>]
[WITH TRUNCATE_ONLY | WITH NO_LOG |
WITH NO_TRUNCATE]

dump_device is the name of the dump device to which the dump is being directed. It is optional only if the WITH TRUNCATE_ONLY clause or the WITH NO_LOG clause is included.

The DUMP TRANsaction command removes committed transactions from the log after they are written to the dump device. DUMP DATABASE, on the other hand does not. If the DUMP TRANsaction command is never used, the transaction log will never be cleared out and will eventually fill up.

For small databases and for the master database, use DUMP TRANsaction WITH TRUNCATE_ONLY after each DUMP DATABASE, in order to clear out the log. Care must be taken when using WITH TRUNCATE_ONLY; if it is used without having backed up the database with DUMP DATABASE, the changes that had been recorded in the transaction log are not recoverable.

The option WITH NO_LOG should only be used when space in the database has totally run out. Immediately after running the DUMP TRANsaction with the WITH NO_LOG option the DUMP DATABASE command should be run because no backup copy of the inactive part of the log is made since there is no space available.

The NO_TRUNCATE option, unlike the TRUNCATE_ONLY and WITH NO_LOG options, does not purge the log of committed transactions.

5. Related Policies

   4.5.14.2 Backup Schedule

   4.5.14.5 Backing Up Databases

6. Bibliography

   Sybase Administration Guide

4.5.14.7 Database Recovery

Responsible Role: Database Administrator

Supporting Role: N/A

1. Frequency

   As needed.

2. Preconditions

   Database device failure or data loss.

3. Goal

   To recover database to its latest backup state.

4. Operating Instructions

If a device in which a user database resides fails and the database is damaged or inaccessible, the database can be restored by reloading the most recent database dump and the succeeding transaction log dumps. Assuming the current log is on an undamaged device, it is dumped with the DUMP TRANsaction command using the NO_TRUNCATE option.

Steps to Recover a Database

A. If the transaction log is on a separate device, use the NO_TRUNCATE option of DUMP TRANsaction to dump the transaction log of the damaged or inaccessible user database.

B. Use the following query to examine the device allocations and uses for the damaged database. The same blocks of space will need to be assigned for the same purposes. This query shows the uses and sizes of the devices allocated to the user database "mydb".

```
select segmap, size
where dbid =
(select dbid
```

from sysdatabases
where name = <"mydb">)

C. Examine the output of the query. Each row with a "3" in the segmap column represents a data allocation; each row with a "4" in the column represents a log allocation. The size column indicates the number of 2K blocks (there are 512 - 2K blocks in a megabyte).

D. If the segmap column contains 7's, this means the database and the transaction log are stored on the same device and recovery is only possible up to the last database or transaction log. The LOG_ON option should not be used with the CREATE DATABASE command when recreating the database (step H.). Make sure sufficient space is allocated. Note the order, use, and size of the output from the query. For example:

Table 4-1

Segmap	Size
3	10240
3	5120
4	5120
3	1024
4	2048

translates into these uses and sizes in megabytes:

Table 4-2

Use	Size
Data	20
Data	10
Log	10
Data	2
Log	4

E. Use the DROP DATABASE command to delete (drop) the database on the failed device. If the system reports errors, use the DROPDB option of the DBCC (Data Base Consistency Checker) DBREPAIR command. (see 4.5.14.8 Using the DBCC command).

F. After the database has been dropped, drop the failed device with sp_drop device.

G. Initialize a new database device with the DISK INIT command.

H. Recreate the database using the CREATE DATABASE command to duplicate all the rows from the old sysusages table, up to and including, the first log device. For the current example the syntax would be:

% CREATE DATABASE <mydb> on
<datadev1> on = 20,
LOG ON <logdev1> = 10

I. Use the ALTER DATABASE command to re-create the rest of the entries. In this example, to allocate more space on datadev1, the command syntax is as follows:

ALTER DATABASE on <datadev1> = 2

When space is allocated on existing devices, it is automatically assigned the same usage: data or log. When space is allocated on a device that is not already in use by the database, it is always allocated as a data device. To recreate the final allocation on logdev1, which is already in use by the database, use the following command:
ALTER DATABASE <mydb> on <logdev1> = 4

It will automatically be entered into the sysusages table as a log device. If space needs to be allocated on a device that is not already in use by the database, the database needs to be altered with the ALTER DATABASE command and followed by the sp_logdevice command as follows:

ALTER DATABASE <mydb> on <logdev1> = 4

It will automatically be entered into the sysusages table as a log device. If space needs to be allocated on a device that is not already in use by the database, the database needs to be altered with the ALTER DATABASE command and followed by the sp_logdevice command as follows:

ALTER DATABASE <mydb> on <logdev2> = 4
sp_logdevice <mydb>, <logdev2>

J. Reload the database using LOAD DATABASE, then load previously dumped logs and the newly-dumped current log using LOAD TRANsaction.

5. Related Policies

4.5.14.8 Using the DBCC (Data Base Consistency Checker) Command

6. Bibliography

Sybase Administration Guide

4.5.14.7.1 Loading a Database

Responsible Role: Database Administrator

Supporting Role: N/A

1. Frequency

   As needed.

2. Preconditions

   A dump database device must be available with the media containing the database to be loaded.

3. Goal

   To load a database from storage media.

4. Operating Instructions

The LOAD DATABASE command is designed for user databases only. The master database is restored with different commands. Loading a database locks it so that no one can modify it while recovery is in process.

If a failure occurs while a database is being loaded, the SQL server does not recover the partially loaded database, but does notify the System Administrator. The database load must be re-started by repeating the LOAD command.

The syntax of the LOAD DATABASE command is:

% LOAD DATABASE <database_name>
FROM dump_device

The database name specified in the command is the name of the database currently in use which will receive the data from the backup copy. It can be a new database with no data in it, or an existing database. Loading data into an existing database overwrites the data in it.

5. Related Policies

   None

6. Bibliography

   Sybase Administration Guide

4.5.14.7.2 Loading Transaction Logs

Responsible Role: Database Administrator

Supporting Role: N/A

1. Frequency

   As needed.

2. Preconditions

   A dump database device must be available with the media containing the database logs to be loaded.

3. Goal

   To load database transaction logs from storage media.

4. Operating Instructions

Loading transaction logs recovers as much of a database as possible in case of a system failure.

The backups of the transaction log must be loaded in the same sequence they were created.

Loading a transaction log dump results in re-execution of the changes it contains and rolling back any uncommitted transactions when the transaction log was dumped. After a transaction log is loaded, the database is in the state it was when the transaction log was dumped, minus any transactions that were still active (not committed) at that time.

The syntax of the LOAD TRANsaction command is:

% LOAD TRANsaction <database_name>
FROM dump_device

LOAD TRANsaction can only be used after a database has been restored from a backup made with the DUMP DATABASE command. Once the database has been reloaded, the transaction log(s) can be loaded.

5. Related Policies

   None

6. Bibliography

   Sybase Administration Guide

4.5.14.7.3 Restoring the Master Database

Responsible Role: Database Administrator

Supporting Role: N/A

1. Frequency

As needed.

2. Preconditions

   A dump database device must be available with the media containing the master data base backup to be loaded.

3. Goal

   To restore a damaged master database from backups.

4. Operating Instructions

The procedure to recover a damaged master database is different than the procedure for recovery of user databases. Signs of a damaged master database are:

Inability to start the SQL server
Segmentation faults
Input/output errors reported by DBCC (Data Base Consistency Checker). (see 4.5.14.8 Using the DBCC command).

It is strongly recommended that the master database be backed up with DUMP DATA BASE each time it is changed. This is accomplished by prohibiting the creation of user defined objects in master and by limiting privileges of the commands that modify it to the Database Administrator. The most common commands that modify the master database are:

DISK INIT
sp_addumpdevice
sp_dropdevice
CREATE DATABASE
ALTER DATABASE
sp_addlogin
sp_droplogin

If the master database is damaged and a device has been added since the last dump (with DISK INIT), the sysdevices table must be rebuilt using the DISK REINIT command.

If the master database is damaged and a database has been created or altered since the last dump (with CREATE DATABASE or ALTER DATABASE), the sysusages and the sysdatabases tables must be rebuilt with the DISK REFIT command. Other changes since the last dump cannot be recovered; they must be reissued on the rebuilt master database.

Steps to Recover the Master Database:

To restore a damaged master database, the Sybase System Administrator must perform the following steps:

A. Build a new master database

The first step is to run:

% buildmaster -m

to replace the damaged master database with a copy of a "generic" master database. (for more information on buildmaster see the Sybase Commands Reference Manual).

B. Load the system procedures by running:

% installmaster

C. If a new dump device is needed, execute sp_addumpdevice with the desired parameters:

D. Restart the SQL server in single user mode as follows:

% startserver -m <RUN_SYBASE>

When the SQL server is started in single user mode, it is automatically configured to allow direct updates to the system tables.

E. Load Master Database Backup:

The next step is to load the most recent backup of master.
After the LOAD DATABASE command has been completed successfully, the SQL server automatically shuts itself down.

If no CREATE DATABASE, ALTER DATABASE, or DISK INIT commands have been issued since the last database dump was made (Check the data base administration log), master is now completely restored.

The SQL server can now be set to multi-user mode and proceed with the operations. To do this restart the server in multi-user mode as follows:

% startserver -f <RUN_SYBASE>

F. If a device has been added since the last dump with the DISK INIT command, use the DISK REINIT command to recover those changes.

G. It is very important to give the correct information when issuing the DISK REINIT command, especially about the size; otherwise the data may be corrupted.

The syntax for DISK REINIT command follows (note that it is almost identical to DISK INIT):

% DISK REINIT
NAME = <"device_name">
PHYSNAME = <"physical_name">,

VDEVNO = <"virtual_device_number">,
SIZE = <number of 2K blocks>

DISK REINIT must be issued from the master database.

H. If DISK REINIT was run, or if CREATE DATABASE or ALTER DATABASE have been used since the last dump, make hard copies of the sysusages and the sysdatabases tables and then issue the DISK REFIT command as follows:

% DISK REFIT

DISK REFIT can only be run by the System Administrator from the master database.

I. After running DISK REFIT, the SQL server needs to be checked carefully:

Compare the hard copy of sysusages and sysdatabases with the new on-line version.

Run DBCC CHECKALLOC on each database (see 4.5.14.8 Using the DBCC command).

Examine important tables in each database.

J. If everything is correct, shutdown the SQL server and restart it in multi-user mode as follows:

% shutdown

% startserver <RUN_SYBASE>-f

If any discrepancies are found in the sysusages table, edit the table to correct the discrepancies.

If other problems are found, the most probable cause is that DISK REINIT was not run or that inaccurate information was used when it was run. Check the information and correct the sysdevices table by re-running DISK REINIT. Then re-issue DISK REFIT.

Changes other than CREATE DATABASE, ALTER DATABASE, and DISK INIT that were made after the last dump of the master database have to be re-issued. Some of these changes can be sp_adduser, sp_dropuser, or system variables changed with sp_sysconfigure and RECONFIGURE.

5. Related Policies

4.5.14.8 Using the DBCC (Data Base Consistency Checker) Command

6. Bibliography

Sybase Administration Guide

4.5.14.8 Using the DBCC (Data Base Consistency Checker) Command

Responsible Role: Database Owner

Supporting Role: Database Administrator

1. Frequency

   As needed.

2. Preconditions

   None.

3. Goal

   To check the logical and physical consistency of a database.

4. Operating Instructions

The Database Owner is automatically granted permission to use the DBCC command and its options.

A. The syntax of the DBCC command is as follows:

% DBCC {CHECKTABLE (<table_name>) |
CHECKDB [(<database_name>)] |
CHECKALLOC [(<database_name>)] |
CHECKCATALOG [(<database_name>)] |
DBREPAIR (, DROPDB)}

DBCC can be run while the database is active, except for the DBREPAIR option.

The CHECKTABLE option checks the specified table to see that index and data pages are correctly linked, indexes are in properly sorted order, all pointers are consistent, and the data on each page and page offsets are reasonable.

The CHECKDB option runs the same checks as CHECKTABLE, but on each table in the specified database. If no database is given, CHECKDB checks the current database.

The CHECKALLOC option checks the specified database to see that all pages are correctly allocated, and no page is allocated that is not used. If no database name is given, CHECKALLOC checks the current database.

The CHECKCATALOG option checks for consistency within and between system tables. For example, it makes sure every type in syscolumns has a matching entry in systypes; every table and view in sysobjects has at least

one column in syscolumns; and the last checkpoint in syslogs is valid. If no database name is given, CHECKCATALOG checks the current database.

The DBREPAIR DROPDB option drops a damaged database. DROP DATA BASE does not work on a damaged database.

No users can be using the database being dropped or repaired when the DBREPAIR is issued. The DBCC command with the DBREPAIR option must be issued from the master database.

5. Related Policies

   4.5.14.7 Database Recovery

   4.5.14.7.3 Restoring the Master Database

6. Bibliography

   Sybase Administration Guide

4.6 IMPLEMENTING PROCEDURES FOR FACILITY THREATS

General procedures for facility threats are outlined in LOPP Volume One, 4.5 Implementing Procedures for Facility Threats. Specific instructions to be followed in the event of a facility threat are contingent upon physical location and respective safety criteria. Specific operational instructions for each facility should be developed by the Facility Manager.

4.7 IMPLEMENTING PROCEDURES FOR SECURITY THREATS

General procedures for security threats are outlined in LOPP Volume One, 4.6 Implementing Procedures for Security Threats. Specific instructions to be followed in the event of a security threat or computer virus are contingent upon security plans. Specific operational instructions for each facility should be developed by the Security Officer.

5 SECURITY

Security for the library presents many challenges. After completing a risk analysis to identify threats, countermeasures are invoked to preclude these threats. This is an on going process and there are many ideas to counter these threats, however at this point no implementation of these countermeasures has occurred. A security plan will be written to map out the implementation of countermeasures. The plan will identify all aspects of countermeasure implementation (i.e., cost vs. risk).

This chapter will continue to be updated as knowledge is gained about countermeasure implementation. Security is an ongoing process that will never be a finished product. Security must be a daily part of the library operation.

6 QUALITY ASSURANCE

This chapter details the quality mechanisms in place to assure the production and maintenance of a quality software storage and integration environment.

Additional quality assurance operating instructions will be written when metric procedures, etc., are clearly defined and we have gained more experience in our operations.

6.1 CONFIGURATION CONTROL BOARD (CCB) PROCESS

Responsible Role: CCB Chairperson.

Supporting Role(s): CCB voting members and attendees.

1. Frequency: As needed.

2. Preconditions: One or more issues (e.g., need for a library release) have arisen requiring a management decision affecting any operational library.

3. Goal: The goal of this procedure is to establish the process to ensure the CCB is a valid check and balance on issues affecting the operational libraries, i.e., all events that could affect an operational library has CCB approval prior to implementation.

4. Operating Instructions:

   A. Chairperson develops and maintains a Charter. This Charter contains at least the following information:

      - List of voting and non-voting people/groups.
      - Roles (e.g., who the Chairperson is) of voting members.
      - Description of the purpose and intent of the CCB.
      - Definition of a quorum.
      - Set of high level procedures.
      - A typical agenda.

   B. Anyone wanting a CCB meeting must see the Chairperson or Recorder to schedule the meeting and to set an agenda.

   C. Chairperson or Recorder will announce all meetings in advance (three work days when possible).

D. Chairperson will appoint a person to prepare and publish minutes for all meetings. Minutes should be published within three work days and be available to the entire Staff.

E. Non-voting people can attend any meeting; but they can only partake when asked to participate by a voting member.

F. For a library release, the following will give a presentation/status:

- LCB Chairperson will summarize why the LCB is presenting the issue to the CCB and any known problems/issues.
- Quality Management/Testing Lead will provide its recommendation (approve/disaprove) and any known problems not addressed by the LCB Chairperson.

6.2 LIBRARY CONTROL BOARD (LCB) PROCESS

Responsible Role: LCB Chairperson.

Supporting Role(s): LCB voting members and attendees.

1. Frequency: Once a week (if possible), or as needed.

2. Preconditions: One or more issues (e.g., need for a library release) have arisen requiring a technical decision affecting the developmental or operational libraries.

3. Goal: The goal of this procedure is to establish the process to ensure the LCB is a valid check and balance on issues affecting the developmental or operational libraries, i.e., all events that could affect a developmental or operational library has LCB approval prior to implementation.

4. Operating Instructions:

A. Chairperson develops and maintains a Charter. This Charter at least contains the following information:

- List of voting and non-voting people/groups.
- Roles (e.g., who the Chairperson is) of voting members.
- Description of the purpose and intent of the LCB.
- Definition of a quorum.

- Set of high level procedures.
- A typical agenda.

B. Anyone wanting an LCB meeting must see the Chairperson or Recorder to schedule the meeting and to set an agenda.

C. Chairperson or Recorderwill announce all meetings in advance (three work days when possible).

D. Recorder will prepare and publish minutes for all meetings. Minutes should be published within three work days and be available to the entire Staff.

E. Non-voting people can attend any meeting; but they can only partake when asked to participate by a voting member.

F. For a library release, the following will give a presentation/status:

- Library Development will provide a summary of the status, including configuration and documentation management, and any known problems/issues.
- Quality Management/Testing Lead will provide its recommendation (approve/disaprove) and any known problems not previously addressed.

6.3 STAFF

Responsible Role: Functional Group Leaders, e.g., System Administrator, Configuration Manager, Facility Manager, Security Officer, and Library Administrator.

Supporting Role(s): Library Staff.

1. Frequency: As needed.

2. Preconditions: None.

3. Goal: To prevent quality problems. If this cannot be met, then to:

   A. Detect and correct any problems prior to the problems affecting Users or the final products.

   B. Identify why the problems occurred and provide feedback so the problems will not occur again.

4. Operating Instructions:

A. Staff members are responsible for their work. As a result, if a problem occurs, the problem will be documented and Staff member(s) will be assigned to correct the problem. Staff members will implement their portion of plans, procedures, etc.

B. Staff members will collect metric data for the Quality Engineers.

C. Staff members will recommend needed process or product improvements to the responsible group(s) and Quality Engineers.

D. Staff members will be assigned to identify the cause(s) of problems and make a recommendation to the Staff on preventing reocurrance of the problems.

E. Functional Group Leaders will ensure procedures are in place, are being followed, periodically reviewed, and updated as needed.

F. Any Library Account Holder can make recommendations to change procedures, products, or services.

G. All Library procedures will be made part of the LOPP, or referenced within the LOPP.

6.4 QUALITY ENGINEER

Responsible Role: Quality Engineer, e.g., CCB and LCB Chairpersons.

Supporting Role(s): Library Staff.

1. Frequency: As needed.

2. Preconditions: None.

3. Goal: To prevent quality problems. If this cannot be met, then to:

   a. Detect and correct any problems prior to the problems affecting Users or the final products.

   b. Identify why the problems occurred and provide feedback so the problems will not occur again.

4. Operating Instructions:

   A. Staff members report metric data and problems (per their problem reporting procedures).

B. Quality Engineers perform periodic audits based on Staff policies, procedures, and operating instructions.

C. Quality Engineers report their findings to the Staff.

D. Problems found with any procedure will result in the procedure being audit by the Quality Engineers within six months of problem discovery.

E. Quality Engineers will develop plans, policies, procedures, operating instructions, etc., so audits can be performed on library procedures, for reporting issues, and for ensuring problems/issues are resolved.

F. Quality Engineers develop and report metric trend analysis to the Staff, along with recommendations.

7 CONFIGURATION MANAGEMENT

The day-to-day procedures for Configuration Management will be published in a Configuration Management Plan. Delivery of the Configuration Management Plan is TBD.

8 INTEROPERATION

Interoperation is defined as the manual and/or automated process of sharing assets between reuse libraries. This definition, though, is misleadingly simple. To interoperate with another library, many differences between the libraries must be resolved, including business policies, legal issues, and technical issues. Even within these rather broad areas, there are numerous levels of issues to address.

This chapter describes operations when dealing with some of these problems. As experience is gained and more libraries are brought into the interoperation arena, better solutions will present themselves, requiring updates to this chapter in both Volume One and Volume Two. Further, as new problems arise and are solved, new sections will undoubtedly need to be added.

When using and reviewing these policies and procedures, one must always keep in mind that interoperation hinges on an agreement between multiple libraries, detailed in a Memorandum Of Understanding ("Memorandum of Understanding among Interoperating Member Libraries of the DoD Software Reuse Initiative Virtual Library", dated 10/20/93, hereafter referred to as "the MOU"). Should the MOU and these operating instructions conflict, the MOU is the governing document. In any case, this document should serve as a guideline for the MOU.

The Interoperability Plan is an informal document detailing the architecture, design and basic operation of interoperability between all cooperating libraries. The CARDS implementation of this architecture is known as the CARDS Library Interoperability System (LIS).

8.1 MAINTAINING INTEROPERATION INDEXES

Responsible Role: CCB Chairperson

Supporting Role(s): Library Administrator, Hotline Operator

1. Frequency

   As assets change (see the Preconditions section for a definition of change).

2. Preconditions

   A change has been made to the set of assets available for interoperability. A change may be any or all of: addition of a new asset, removal of an existing asset, and/or update of an existing asset. (This typically occurs when a new version of the CARDS library is released).

3. Goal

   To ensure that complete and consistent indexes are available for asset interchange among cooperating (interoperating) Library Systems.

4. Operating Instructions

A. CCB Chairperson - inform the Library Administrator of new assets being made available, old assets being removed, and/or changes to existing assets

- Send a memo to the Library Administrator, identifying the changes being made and their effective date.

B. Library Administrator - notify cooperating librarians of impending changes to assets

- Determine asset changes that will affect cooperating libraries.
- Have the Hotline Operator send electronic mail to notify affected cooperating libraries detailing the changes to be made.

C. Library Administrator - install revised index

- Edit the local index as required.
- Determine how much advance notice is required to the cooperating libraries before the index can be installed.
- After waiting for the required period, install the local index.

D. Library Administrator - notify cooperating librarians of change in index

- Determine how much advance notice is required for the particular changes being made to the local index. This is defined in the MOU, Section 5.1, "Index Change Notification".
- Have Hotline Operator send electronic mail to notify cooperating librarians that the new index is installed.
- Formally notify the LCB Chairperson and the CCB Chairperson that the new index is installed via memo or electronic mail.

5. Related Policies

None

6. Bibliography

Interoperability Plan

8.2 INSTALLING THE LIBRARY INTEROPERABILITY SYSTEM

Responsible Role: Library Administrator

Supporting Role(s): Hotline Operator, System Administrator

1. Frequency

   As needed.

2. Preconditions

   A new/different LIS will need to be installed if this condition is met:

   - A new version of the LIS is released due to repaired defects, expanded functionality, or other updates from the Library Development Team.

     Note that, if a new version of the CARDS library is installed, the LIS will automatically be installed as part of that procedure, and this procedure does not need to be executed.

3. Goal

   To ensure accurate and complete installation of new and revised implementations of programmatic interoperation services.

4. Operating Instructions

   A. Library Administrator - make request for LIS installation

      - See the section on System Software Installation/Upgrade. The new/different version of the LIS should be explicitly identified to the System Administrator, as well as the reason for the installation.

      - Through coordination with the System Administrator, determine the optimum date and time for the installation.

   B. Library Administrator - inform cooperating libraries of impending installation, including the reasons and date. This step may be skipped in the case of an emergency installation. An emergency installation is defined as an installation of a new/different LIS which is being performed to (a) protect the security of the libraries and its associated hardware and software assets, and/or (b) correct mission critical or excessive defects that prevent the correct operation of the LIS and libraries. Under no other circumstances can an installation be deemed an emergency.

- Have the Hotline Operator send electronic mail to notify cooperating librarians of the date of and reason for the impending installation.

C. System Administrator - install a new/different LIS

- With the Library Administrator, set a date and time for the installation of the LIS.
- Install the LIS as per instructions supplied by the Library Development Team.
- Start the LIS.
- Notify the Library Administrator of successful installation.

D. Library Administrator - inform cooperating librarians of completed LIS installation

- Within one hour of LIS installation, have the Hotline Operator send electronic mail to notify cooperating librarians of installation of LIS.

5. Related Policies

4.1 SOFTWARE INSTALLATION AND UPGRADE

8.2 INSTALLING THE LIBRARY INTEROPERABILITY SYSTEM

6. Bibliography

None

8.3 LIS SERVICE INTERRUPTION

Occasionally, the LIS may be rendered inoperative. The causes can be server program faults, hardware faults, network faults, power failures, etc. This operating instruction is intended to re-establish interoperation services with minimal impact on users and cooperating Library Systems.

As the interface between users and the Library, the Hotline Operator will be the first person who knows of problems encountered by Users. Some basic checks can be made immediately.

Responsible Role: Library Administrator

Supporting Role(s): Hotline Operator, System Administrator

1. Frequency

As needed.

2. Preconditions

A failure or malfunction of the LIS is identified by a user or developer executing the system or through review of the log files.

3. Goal

To ensure timely re-establishment of interoperation services among cooperating Library Systems.

4. Operating Instructions

A. Hotline Operator - upon detection of disruption of LIS services, notify other personnel

- Immediately notify the System Administrator and the Library Administrator in person or via phone.

B. Hotline Operator - perform first level diagnoses of problem

- Test to determine that the machines are reachable.
- Attempt to access the remote asset. In the event of failure, record the error message given by the LIS.
- If either of the above fail, contact the System Administrator with details of the problem.
- If both work and the user again fails to extract the asset, contact the System Administrator.
- If the System Administrator is required to intervene, follow-up with the customer after repairs are effected.

C. System Administrator - upon detection of disruption of LIS services, notify other personnel

- Upon detection of disruption of LIS services, immediately notify the Hotline Operator and the Library Administrator.

D. Library Administrator - notify the cooperating libraries of the problem

- Have the Hotline Operator send electronic mail to notify cooperating librarians of the problem.

E. System Administrator - further diagnose the LIS problem

- If the LIS faulted (core dumped):

  Move the core file to a new subdirectory.

  Copy the LIS log file to the same subdirectory.

  Contact the Library Development team, notifying them of the core and log file.

- If the LIS simply stopped for undetermined reasons:

  Save the LIS log file to a new subdirectory.

  Contact the Library Development Team, notifying them of the log file.

- If the LIS is still functioning properly:

  Gracefully kill the LIS, as per the Library Development Team.

  Restart the LIS.

  Attempt to extract an asset from a cooperating library.

- If the LIS still does not function properly, check for other system problems affecting the LIS. See Chapter 4, Computer Resources. If the system resources are working properly, seek help from the Library Development Team as necessary.

- Update this procedure to reflect new insights and techniques.

F. System Administrator - Restore LIS operation

- Depending on the diagnoses, one of the following will be necessary:

  Repair/restore system resources.

  Manually restart the LIS.

  Reboot the LIS server machine.

  Contact the Library Administrator, requesting an emergency installation of a different LIS.

- Update this procedure to reflect new options and techniques.

G. Library Administrator - notify the cooperating libraries that the problem was resolved

- Have the Hotline Operator send electronic mail to notify cooperating librarians that the problem has been resolved.

5. Related Policies

   4.3 UNIX ADMINISTRATION

   8.2 INSTALLING THE LIBRARY INTEROPERABILITY SYSTEM

6. Bibliography

   None

8.4 MAINTAINING INTEROPERATION NOTIFICATIONS

Responsible Role: System Administrator

Supporting Role(s): Hotline Operator

1. Frequency

   Daily.

2. Preconditions

   None.

3. Goal

   To ensure that Library Users' requests for assets via the LIS are being serviced in a timely fashion, and to ensure high levels of customer satisfaction.

4. Operating Instructions

   A. System Administrator - determine if the LIS is serving users properly

   - Check the notification log daily.
   - If results indicate that some requested assets were not properly delivered, contact the Hotline Operator via electronic mail. Include the user, the asset the user was attempting to extract, and when the attempt was made.

   B. Hotline Operator - determine if the LIS is serving users properly

   - Extract the asset. If the asset is NOT extractable, initiate procedures for a failure in LIS operation.
   - Contact the user and offer assistance.

5. Related Policies

8.3 LIS SERVICE INTERRUPTION

6. Bibliography

Interoperability Plan

8.5 MAINTAINING INTEROPERATION MOU

Responsible Role: Library Administrator

Supporting Role(s): Cooperating Library Administrators

1. Frequency

As needed.

2. Preconditions

A policy or operational change is made that could affect cooperating libraries.

3. Goal

To ensure that interoperation agreements established between/among reuse libraries, as formalized in the Memorandum Of Understanding (MOU), are implemented by the local library.

4. Operating Instructions

A. Library Administrator/Cooperating Library Administrators - determine if a change is necessary to the MOU

- Review the MOU(s) to determine if a change will affect the previously agreed upon policies and procedures.

B. Library Administrator - draft necessary changes

- With the Cooperating Library Administrators, draft a mutually agreeable update to the MOU.
- Submit the update to the CCB.
- Notify the Cooperating Library Administrators of expected verdict from CCB.

C. Library Administrator - notify Cooperating Library Administrators of acceptance or failure of changes

- Formally notify the Cooperating Library Administrators of the verdict via letter. Identify when the expected change will be effective. Request confirmation of receipt of the letter.

- If the change was rejected, iterate between this and the previous step to resolve the reason for rejection.

D. Library Administrator - commence changes that prompted the update to the MOU

- As required by the changes.

E. Library Administrator - notify Cooperating Library Administrators of completion of changes

- Formally notify the Cooperating Library Administrators that the change is complete via letter. At this point, the new MOU is in effect.

5. Related Policies

4.1 SOFTWARE INSTALLATION AND UPGRADE

6. Bibliography

Interoperability Plan

9 METRICS

The metrics chapter outlines the collection and analysis of information that is useful in predicting trends and improving library service and operations.

The following areas are covered in this chapter:

Metrics Definition Change Process

User Support Metrics

System Metrics (User Account, Hardware, Software and Telecommunications)

Interoperability Metrics

Domain Metrics

Component Evaluation Metrics

Component Reuse Metrics

Training Metrics

Library Documentation Metrics

Metrics Analysis and Presentation Process

Implementing Metrics Analysis Results Process

9.1 METRICS DEFINITION CHANGE PROCESS

Responsible Role: Library Administrator

Supporting Role(s): System Administrator

1. Frequency

   The Metrics Implementation Plan (MIP) for Library Operations shall be updated as needed and reevaluated for completeness and usefulness on a regular basis.

2. Preconditions

   Analysis of metrics collected recommends changes to metrics to more truly reflect current operations or to gain further insight into processes and/or products and services.

3. Goal

   The goal of this process is to maintain an up-to-date list of metrics for the Library. What metrics are currently selected? Are metrics providing the answers to our questions? What additional metrics are needed? Where? Are metrics easy (cost-effective) to collect? Is the metrics collection procedure appropriate?

4. Operating Instructions

   A. The Library Administrator maintains a list of metrics to be collected by Library Staff. The Metrics Implementation Plan outlines the six-step process for defining and implementing metrics. As metrics are found to be useful, they are transferred to the LOPP volumes I and II.

   B. Metrics shall be evaluated periodically to determine whether the appropriate information is being gathered.

5. Related Policies

   9.2 USER SUPPORT METRICS

   9.3 SYSTEM METRICS - USER ACCOUNTS

   9.4 SYSTEM METRICS - HARDWARE

   9.5 SYSTEM METRICS - SOFTWARE

   9.6 SYSTEM METRICS - TELECOMMUNICATIONS

   9.7 INTEROPERABILITY METRICS

   9.8 DOMAIN METRICS

   9.9 COMPONENT EVALUATION METRICS

   9.10 COMPONENT REUSE METRICS

   9.11 COLLECTION OF METRICS - TRAINING

   9.12 LIBRARY DOCUMENTATION METRICS

   9.13 METRICS ANALYSIS AND PRESENTATION PROCESS

   9.14 IMPLEMENTING METRICS ANALYSIS RESULTS PROCESS

6. Bibliography

   None

9.2 USER SUPPORT METRICS

Responsible Role: Library Administrator

Supporting Role(s): Hotline Operator

1. Frequency

   Weekly.

2. Preconditions

Metrics pertaining to User Support Functions and Library Accounts are collected.

3. Goal

The goal of User Support is to maintain the highest level of user satisfaction with the library. Who are the current users? What kind of assistance do they need? Are users satisfied with the assistance provided? Is the type of assistance needed changing over time? What are the problems and where are they? Are the components easy to access? Is the access time satisfactory? Is the system useful? What library resources are needed to support users (non-system measures)? What expectations do users have of the Library?

4. Operating Instructions

A. The Hotline Operator collects information pertaining to User Accounts and Hotline Support. Most of this information is collected and recorded in the Hotline Log.

Hotline Support is the most direct interface between CARDS and the user, and, accordingly, directly reflects on user satisfaction. Pertaining to practicality, Hotline support metrics require low personnel and time requirements.

CARDS Staff will be informed of the number and identity of users, and user access to the CARDS Library.

B. The information collected for user accounts is:

- Number of total incoming CLARF's (both staff and users).
- Number of CLARF's approved, disapproved, and returned for more information.
- Average CLARF turnaround time (in days).
- Number of deactivated accounts (due to inactivity or user request).

C. Information is gathered from User Queries (questionnaires, interviews), Hotline Reports, and Weekly User Support Reports. The collection schedule shall be weekly which is then compiled into a monthly report. A statistical measurement gauge is applied to the results. The optimum level for Average CLARF turnaround time has been set at 2.5 days. The optimum level for the number of deactivated accounts is 0. The critical level for average CLARF turnaround time is 5 days. The critical level for the number of deactivated accounts has been set at one.

D. User Account Metrics are related to other metrics. They will have a direct impact on training. Also, if a user is not satisfied with knowledge given through training, the number of account deactivations could go above the critical level.

E. The information collected for hotline support is:

- Number of hotline calls:

  Phone

  E-mail

  Wrong numbers

  Time of peak activity

- Number of outgoing calls:

  Phone follow-up calls

  E-mail follow-up messages

  Acknowledgment messages

- Hotline Reports for staff:

  Hardware

  Software

  Interface

  Policy

  Components

  User Error

- Hotline Reports for Users:

  Hardware

  Software

  Interface

  Policy

  Components

  User Error

- Customer Hotline Reports

- Hotline response time:

  (1) Hotline Staff Reports:

  Hardware

  Software

  Interface

  Policy

  Components

  User Error

  (2) Hotline User Reports:

  Hardware

  Software

  Interface

  Policy

  Components

  User Error

- Was the CARDS staff able to answer your questions?

- Was the CARDS staff able to answer your questions completely?

F. User Support uses Hotline Support metrics to track problem resolution, to evaluate problem resolution by each team, to pinpoint problem areas which need attention (i.e., hardware, software), and to identify the effectiveness of communication among CARDS teams. For example, metrics collected from Hotline Reports will show the specific user problem (hardware, software, RLF-GB, Operator Error), the time required for resolution, and the number of user calls to the hotline. This information helps CARDS Staff determine the overall performance of the system.

G. Hotline data is gathered and evaluated. A statistical measurement gauge and a Likert Scale (1=Poor, 5=Good) is applied. The optimum level is no problems. The critical level is TBD.

Hotline Support Metrics are related to other metrics. Because most inquiries about CARDS go through the Hotline, Hotline Metrics will have a direct impact on all User Support Metrics.

5. Related Policies

9.1 METRICS DEFINITION CHANGE PROCESS

9.3 SYSTEM METRICS - USER ACCOUNTS

9.4 SYSTEM METRICS - HARDWARE

9.5 SYSTEM METRICS - SOFTWARE

9.6 SYSTEM METRICS - TELECOMMUNICATIONS

9.7 INTEROPERABILITY METRICS

9.8 DOMAIN METRICS

9.9 COMPONENT EVALUATION METRICS

9.10 COMPONENT REUSE METRICS

9.11 COLLECTION OF METRICS - TRAINING

9.12 LIBRARY DOCUMENTATION METRICS

9.13 METRICS ANALYSIS AND PRESENTATION PROCESS

9.14 IMPLEMENTING METRICS ANALYSIS RESULTS PROCESS

6. Bibliography

None

9.3 SYSTEM METRICS - USER ACCOUNTS

Responsible Role: Library Administrator

Supporting Role(s): System Administrator

1. Frequency

Daily, Weekly and Monthly.

2. Preconditions

System metrics pertaining to User Accounts are collected automatically by the system as users interact with it.

3. Goal

The goal of this procedure is to collect system metrics pertaining to user accounts. Who are the users? How many users are there? How often and how long do they used the system? What communications means do they use? What disk storage is required for local net versus remote operation? What aspects of the Library do they use most often? Least? Never? Why? What security breeches have occurred and why?

4. Operating Instructions

   A. To collect the account disk usage by user type the System Administrator must run the "acct_disk_usg.metrics" shell script. The format of the command is:

      acct_disk_usg.metrics begin_date end_date

   B. To collect information about connect time for remote logins via telnet, number of remote logins via telnet, connect time running the RLF-GB, and the number of times the RLF-GB is run, the System Administrator would execute the command:

      rmt_cnt.metrics begin_date end_date

   C. If merited by the metrics, the Library Administrator suggests system hardware and software acquisitions to the CCB to keep pace with system usage and predictions. The System Administrator routinely makes suggestions to improve the system efficiency to the Library Administrator. Suggestions are also presented to the CCB.

5. Related Policies

   9.1 METRICS DEFINITION CHANGE PROCESS

   9.2 USER SUPPORT METRICS

   9.4 SYSTEM METRICS - HARDWARE

   9.5 SYSTEM METRICS - SOFTWARE

   9.6 SYSTEM METRICS - TELECOMMUNICATIONS

   9.7 INTEROPERABILITY METRICS

   9.8 DOMAIN METRICS

   9.9 COMPONENT EVALUATION METRICS

   9.10 COMPONENT REUSE METRICS

   9.11 COLLECTION OF METRICS - TRAINING

   9.12 LIBRARY DOCUMENTATION METRICS

   9.13 METRICS ANALYSIS AND PRESENTATION PROCESS

   9.14 IMPLEMENTING METRICS ANALYSIS RESULTS PROCESS

6. Bibliography

   None

9.4 SYSTEM METRICS - HARDWARE

Responsible Role: Library Administrator

Supporting Role(s): System Administrator

1. Frequency

   Daily, Weekly and Monthly.

2. Preconditions

   System metrics for system hardware are collected.

3. Goal

   The goal of this procedure is to collect system metrics for system hardware. What is the current system performance? What are the bottlenecks? What system hardware will be required to maintain an adequate level of system performance? When will hardware additions need to be ordered and installed?

4. Operating Instructions

   A. At present, metrics information about system downtime, disk and CPU usage is collected. The disk usage is categorized by file system to illustrate needs for repartitioning of the disk. This information is graphically represented showing used and free space. To collect the information, the System Administrator runs a CARDS created shell script using the command:

      fs_disk_usg.metrics

   B. To collect information about the CPU usage, the System Administrator types the command:

      cpu_usage.metrics begin_date end_date

   C. For "planned" downtime, the System Administrator gathers information about the kind of downtime (maintenance, backups, software installation, etc.) and its planned vs actual duration. This information is kept in the downtime log on a per server basis.

   D. The Library Administrator provides periodic reports to the CCB about the status of system utilization, using metrics to illustrate trends. Hardware acquisitions are suggested to keep pace with the growth of the computing base. Suggestions from the System Administrator are incorporated into the presentation.

5. Related Policies

9.1 METRICS DEFINITION CHANGE PROCESS

9.2 USER SUPPORT METRICS

9.3 SYSTEM METRICS - USER ACCOUNTS

9.5 SYSTEM METRICS - SOFTWARE

9.6 SYSTEM METRICS - TELECOMMUNICATIONS

9.7 INTEROPERABILITY METRICS

9.8 DOMAIN METRICS

9.9 COMPONENT EVALUATION METRICS

9.10 COMPONENT REUSE METRICS

9.11 COLLECTION OF METRICS - TRAINING

9.12 LIBRARY DOCUMENTATION METRICS

9.13 METRICS ANALYSIS AND PRESENTATION PROCESS

9.14 IMPLEMENTING METRICS ANALYSIS RESULTS PROCESS

6. Bibliography

None

9.5 SYSTEM METRICS - SOFTWARE

Responsible Role: Library Administrator

Supporting Role(s): System Administrator

1. Frequency

As needed, at least monthly.

2. Preconditions

Software metrics are collected to evaluate software uptime, quality, and reliability of the library software.

3. Goal

The goal of this metric is to measure the availability, quality and reliability of library software. What bugs are in the Library Software? How many Software Trouble Reports (STR) are being reported? How many problems result in unplanned system downtime? What is the impact on usability? Are the STRs decreasing or increasing? How quickly are STRs closed?

4. Operating Instructions

   A. Trouble Reports to the hotline are the primary means of measuring defects in on-line software. The number and type of Hotline trouble requests will be tracked and reported. An increase just after a new release of library software is expected as long as the increase is comparable but lower than what was reported in the previous release. Tracking of defects during testing is required for internal quality measurement but is not reported.

   B. Software Change Requests (SCRs) indicate the rate of change of system design. Analysis of SCRs requires a detailed knowledge of the system design. A large number of changes due to a policy or other external change is to be expected. SCRs by users could indicate a serious problem and must be considered and tracked.

5. Related Policies

   9.1 METRICS DEFINITION CHANGE PROCESS

   9.2 USER SUPPORT METRICS

   9.3 SYSTEM METRICS - USER ACCOUNTS

   9.4 SYSTEM METRICS - HARDWARE

   9.6 SYSTEM METRICS - TELECOMMUNICATIONS

   9.7 INTEROPERABILITY METRICS

   9.8 DOMAIN METRICS

   9.9 COMPONENT EVALUATION METRICS

   9.10 COMPONENT REUSE METRICS

   9.11 COLLECTION OF METRICS - TRAINING

   9.12 LIBRARY DOCUMENTATION METRICS

   9.13 METRICS ANALYSIS AND PRESENTATION PROCESS

   9.14 IMPLEMENTING METRICS ANALYSIS RESULTS PROCESS

6. Bibliography

   None

9.6 SYSTEM METRICS - TELECOMMUNICATIONS

Responsible Role: Library Administrator

Supporting Role(s): System Administrator

1. Frequency

   As needed.

2. Preconditions

   Telecommunications data is collected daily for each link.

3. Goal

   The goal of telecommunications metrics is to monitor and improve communications resource utilities. What telecommunications systems are users using? Is the system reliable and responsive? Is the bandwidth adequate? What is the average response time across the network? What problems exist with the Internet, the gateway, and the CSU/DSU?

4. Operating Instructions

   A. The System Administrator collects metrics information pertaining to LAN and WAN telecommunications (e.g., average response time across the network, number of remote logins and connect time, number of packets and number of packet collisions, number of line disconnects, downtime per link, and link error rates, etc.) as applicable.

   B. The Library Administrator presents the telecommunications metrics to the CCB. Communication problems may indicate a need for trouble reports to service provider, upgrading communications hardware and/or bandwidth. Trends are illustrated and library improvements are suggested.

5. Related Policies

   9.1 METRICS DEFINITION CHANGE PROCESS

   9.2 USER SUPPORT METRICS

   9.3 SYSTEM METRICS - USER ACCOUNTS

   9.4 SYSTEM METRICS - HARDWARE

   9.5 SYSTEM METRICS - SOFTWARE

   9.7 INTEROPERABILITY METRICS

   9.8 DOMAIN METRICS

   9.9 COMPONENT EVALUATION METRICS

   9.10 COMPONENT REUSE METRICS

9.11 COLLECTION OF METRICS - TRAINING

9.12 LIBRARY DOCUMENTATION METRICS

9.13 METRICS ANALYSIS AND PRESENTATION PROCESS

9.14 IMPLEMENTING METRICS ANALYSIS RESULTS PROCESS

6. Bibliography

None

9.7 INTEROPERABILITY METRICS

Responsible Role: Library Administrator

Supporting Role(s): Component Engineer, Hotline Operator

1. Frequency

Daily, Weekly and Monthly analysis.

2. Preconditions

Usage and performance metrics for interoperation are collected continuously.

3. Goal

The goal of collecting interoperability metrics is to assess the effects of interoperability on their respective library operations. How many assets are available for extraction in relation to the entire asset catalog? How many abstract requests and extractions were cross-library, and what is the efficiency of these transfers? What are the available assets? How many searches are done? How many requests are made for assets and abstracts? What are the effects of interoperability on their respective libraries?

4. Operating Instructions

Measurements are broken into four groups: available assets (local and remote), searches, abstract requests (local and remote), and asset requests (local and remote)

All metric information is collected and stored in two log files: asset information for static metrics, and library usage for dynamic metrics.

A. The following information is collected automatically through a shell script for all local and remote assets:

the originating library

the unique ID of the asset

size of asset

size of the assets's abstract in bytes

asset title

B. The number of searches performed, and the number of hits resulting from these searches is only collected for "foreign" libraries. CARDS does not support structured, query-based searches.

C. The following information will be collected through the display action script for all local and remote abstract requests:

the originating library

the User's ID (or AFS user name)

the date and time when the abstract was requested

time from abstract request to time to call the request mechanism

the asset UID

the asset title

D. The following information will be collected for local and remote assets:

library name

the user name (or AFS name)

date and time the information was logged

time to copy files from the Library's storage to the User's directory

node name and title

asset UID

E. The Library Administrator produces an internal, weekly metrics report showing the available assets by library, the number of local and remote successful and unsuccessful abstract requests, and the number of local and remote successful and unsuccessful asset requests. This weekly report is rolled into a monthly report for distribution.

F. The Hotline Operator counts the number of errors encountered by the user, including corrupt components and descriptions, and inability to retrieve components. The collection of the information is dependent upon the users notifying the CARDS Hotline when any of these events occur.

5. Related Policies

9.1 METRICS DEFINITION CHANGE PROCESS

9.2 USER SUPPORT METRICS

9.3 SYSTEM METRICS - USER ACCOUNTS

9.4 SYSTEM METRICS - HARDWARE

9.5 SYSTEM METRICS - SOFTWARE

9.6 SYSTEM METRICS - TELECOMMUNICATIONS

9.8 DOMAIN METRICS

9.9 COMPONENT EVALUATION METRICS

9.10 COMPONENT REUSE METRICS

9.11 COLLECTION OF METRICS - TRAINING

9.12 LIBRARY DOCUMENTATION METRICS

9.13 METRICS ANALYSIS AND PRESENTATION PROCESS

9.14 IMPLEMENTING METRICS ANALYSIS RESULTS PROCESS

6. Bibliography

None

9.8 DOMAIN METRICS

Responsible Role: Library Administrator

Supporting Role(s): Component Engineer

1. Frequency

As needed.

2. Preconditions

Domain metrics are collected for component evaluation.

3. Goal

Domain metrics are used to evaluate components based on domain requirements, architectural constraints, and implementation constraints. What components are in the domain model? What is the domain model configuration? What resources does it need? What is the degree to which the domain model is fully populated with components?

Since the scope of this document is the maintenance of an existing library, Domain Metrics are explained in more detail in the Library Development Handbook [CARDS93h]

4. Operating Instructions

   A. The LCB chair maintains a list of Domain Metrics for evaluation of incoming components.

   B. The list shall be reevaluated on a regular basis and kept current. There shall be a separate list of metrics for each domain being examined.

5. Related Policies

   9.1 METRICS DEFINITION CHANGE PROCESS

   9.2 USER SUPPORT METRICS

   9.3 SYSTEM METRICS - USER ACCOUNTS

   9.4 SYSTEM METRICS - HARDWARE

   9.5 SYSTEM METRICS - SOFTWARE

   9.6 SYSTEM METRICS - TELECOMMUNICATIONS

   9.7 INTEROPERABILITY METRICS

   9.9 COMPONENT EVALUATION METRICS

   9.10 COMPONENT REUSE METRICS

   9.11 COLLECTION OF METRICS - TRAINING

   9.12 LIBRARY DOCUMENTATION METRICS

   9.13 METRICS ANALYSIS AND PRESENTATION PROCESS

   9.14 IMPLEMENTING METRICS ANALYSIS RESULTS PROCESS

6. Bibliography

   None

9.9 COMPONENT EVALUATION METRICS

Responsible Role: Library Administrator

Supporting Role(s): Component Engineer

1. Frequency

As needed.

2. Preconditions

   Quality factors (also known as Common Metrics or Component evaluation metrics) must be built into the software to be evaluated.

3. Goal

   The goal of component evaluation is to make an objective recommendation concerning the inclusion of a software product into the Library. Since the scope of this document is the maintenance of an existing Library, Component Evaluation is explained in more detail in the Library Development Handbook [CARDS93h]. Do components meet the established standards? What additional software is needed in conjunction with a component? How long has the component been released? Is there a list of known problems? Has the component been field tested? What component sources have been explored? Are all possible sources explored? What resources are needed to evaluate components? What components are in the library and in-the-pipeline? How long does it take to establish evaluation criteria? How long does it take to evaluate a component?

4. Operating Instructions

   A. The LCB Chair person maintains a list of quality factors for evaluation of incoming components. Procedures associated with Component Evaluation Metrics are documented in the Library Development Handbook [CARDS93h].

   B. Component Engineer logs time and materials used in the evaluation for GOTS versus COTS.

   C. The Component Engineer documents and announces updates of the component collection.

5. Related Policies

   9.1 METRICS DEFINITION CHANGE PROCESS

   9.2 USER SUPPORT METRICS

   9.3 SYSTEM METRICS - USER ACCOUNTS

   9.4 SYSTEM METRICS - HARDWARE

   9.5 SYSTEM METRICS - SOFTWARE

   9.6 SYSTEM METRICS - TELECOMMUNICATIONS

   9.7 INTEROPERABILITY METRICS

9.8 DOMAIN METRICS

9.10 COMPONENT REUSE METRICS

9.11 COLLECTION OF METRICS - TRAINING

9.12 LIBRARY DOCUMENTATION METRICS

9.13 METRICS ANALYSIS AND PRESENTATION PROCESS

9.14 IMPLEMENTING METRICS ANALYSIS RESULTS PROCESS

6. Bibliography

None

9.10 COMPONENT REUSE METRICS

Responsible Role: Library Administrator

Supporting Role(s): Component Engineer

1. Frequency

Daily, Weekly and Monthly.

2. Preconditions

Component reuse data are collected continuously.

3. Goal

The goal of this procedure is to collect component usage metrics. These metrics are used to evaluate and improve the usefulness of a Library component to the user, to identify high-value components, and to prioritize selective improvements to be added to the Library. What components are in the library? What components are useful to the users? What components are rejected by the users? What components are needed but not part of the library? What components are in the library and needed by the user but not found?

4. Operating Instructions

A. After component usage metrics information has been compiled and analyzed, the Library Administrator presents a summary at regular LCB meetings. Trends and areas that need improvement are pointed out. Components that are frequently accessed are illustrated as being in a desirable category and suggestions are made concerning other components that may also be just as desirable. Components that are infrequently accessed, or viewed and infrequently retrieved, are

illustrated and recommendations are made concerning the reasons for lack of interest on the part of the users. Projections are made concerning the interests of the Library's growing user base.

B. The Component Engineer collects metrics pertaining to component usage, such as failed queries, component retrieval frequency, and component access frequency.

C. Information feasible to collect at the date of this publication includes: components retrieved, components viewed, and the duration of runs of the RLF.

D. The frequency of requests for retrieving components is accomplished by adding a line to the "extract_files.sh" script that performs the request on behalf of the user. The line added echoes the username, the component name and the date/time to a file in an insert only directory under the AFS. The inserted line looks like:

```
echo "'whoami' extracted file" $LIB_LOC/$i "into"
$TARGET_DIR/$NODE_NAME "on 'date' ">>
afs/cards/Library/component_metrics/EXTRACTED_COMPONENTS/
'date+%a%m%d'
```

The file generated has a unique filename for each day. Subsequent extractions append to the end of the file. The file keeps a journal of all extractions on a particular day. The files are concatenated together at regular intervals and examined to reveal trends about the frequency of component extractions.

Information about viewed components are collected in a similar fashion. The frequency of requests for retrieving remote components is accomplished by adding a line to the "view_description.sh" script that performs the request on the behalf of the user. The line added would echo the username, the component name and the date/time to a file in an insert only directory under the AFS. The inserted line looks like:

```
echo "'whoami' viewed file" $1 "on 'date' ">>
afs/cards/Library/component_metrics/VIEWED_COMPONENTS/'date
+%a%m%d%'
```

The file generated would have a unique filename for each day. Subsequent viewings append to the end of the file. The file keeps a journal of all viewings on a particular day. The files are concatenated together at regular intervals and examined to reveal trends about which components are frequently / infrequently viewed.

E. When deemed necessary by the Library Administrator, the files containing the information concerning which components were viewed and retrieved are

printed by the Component Engineer. They are examined with retrievals and viewings organized by category. Trends are illustrated.

5. Related Policies

9.1 METRICS DEFINITION CHANGE PROCESS

9.2 USER SUPPORT METRICS

9.3 SYSTEM METRICS - USER ACCOUNTS

9.4 SYSTEM METRICS - HARDWARE

9.5 SYSTEM METRICS - SOFTWARE

9.6 SYSTEM METRICS - TELECOMMUNICATIONS

9.7 INTEROPERABILITY METRICS

9.8 DOMAIN METRICS

9.9 COMPONENT EVALUATION METRICS

9.11 COLLECTION OF METRICS - TRAINING

9.12 LIBRARY DOCUMENTATION METRICS

9.13 METRICS ANALYSIS AND PRESENTATION PROCESS

9.14 IMPLEMENTING METRICS ANALYSIS RESULTS PROCESS

6. Bibliography

None

9.11 COLLECTION OF METRICS - TRAINING

Responsible Role: Training Coordinator

Supporting Role(s): Hotline Operator

1. Frequency

At each training session.

2. Preconditions

User data pertaining to training are collected immediately following training courses, and after trainees have been able to use the Library on their own.

3. Goal

The goal of this procedure is to improve training. What common/baseline training is useful to user, library and other staff? What position specific training is needed? Does training address the needs of library users? Is the training effective? Are users who need training getting it? What additional training needs exist? Is feedback used to improve the process?

4. Operating Instructions

The Training Coordinator collects information about the training that CARDS provides.

A. User Support team personnel are responsible for collecting the information from user questionnaires, interviews, and hotline reports. Inputs are obtained immediately following user training sessions and during hotline follow-ups.

B. Hotline questions and user errors are analyzed for areas needing improvement, emphasis and update education.

C. The information collected is as follows:

- Number of training sessions
- Number of attendees
- Trainee background (1=poor, 5=good)
  - 1 - UNIX
  - 2 - Reuse knowledge
  - 3 - AFS
  - 4 - Interface (RLF-GB)
  - 5 - Other tools (ArborText, etc.)
- Performance of on-the-job tasks
  - 1 - Specify systems/software
  - 2 - Code software
  - 3 - Verify systems/software
  - 4 - Use software
  - 5 - Design systems/software
  - 6 - Test systems/software
  - 7 - Control systems/software

8 - Manage systems/software

9 - Other

- The training course was:

  1 - Too short

  2 - Too long

- The material covered was:

  1 - Too specific

  2 - Too general

  3 - Adequate

- Will you be able to apply the course material when using the system?
- Do the examples help to clarify the concepts?
- Were the course handouts useful?
- Would you recommend attendance to your colleagues?
- Would you like to receive additional information?
- What course modifications do you recommend?

D. The above information is gathered and evaluated. A Likert scale (1=poor, 5=good), a binary scale, or an objective measurement is applied. The optimum level is 5 for the Likert scale and Yes for the binary questions. The objective measurement should be "Trainee Satisfaction". The critical level is 3 for the Likert scale and No for the binary questions. The objective critical level would be "Trainee Dissatisfaction".

E. Training Metrics are related to other User Support metrics and will directly affect Hotline Support metrics. If training is not performed to the necessary level, users either will call the CARDS Hotline continually to determine answers to very basic questions or worse, give up on use of CARDS.

5. Related Policies

   9.1 METRICS DEFINITION CHANGE PROCESS

   9.2 USER SUPPORT METRICS

   9.3 SYSTEM METRICS - USER ACCOUNTS

9.4 SYSTEM METRICS - HARDWARE

9.5 SYSTEM METRICS - SOFTWARE

9.6 SYSTEM METRICS - TELECOMMUNICATIONS

9.7 INTEROPERABILITY METRICS

9.8 DOMAIN METRICS

9.9 COMPONENT EVALUATION METRICS

9.10 COMPONENT REUSE METRICS

9.12 LIBRARY DOCUMENTATION METRICS

9.13 METRICS ANALYSIS AND PRESENTATION PROCESS

9.14 IMPLEMENTING METRICS ANALYSIS RESULTS PROCESS

6. Bibliography

None

9.12 LIBRARY DOCUMENTATION METRICS

Responsible Role: Library Administrator

Supporting Role(s): Hotline Operator

1. Frequency

As needed.

2. Preconditions

Documents are distributed by ASSET and CARDS hotline and are also available on-line. The number of copies distributed are tracked to study reuse library interest.

3. Goal

Library Documentation Metrics help evaluate the understandability, usability, and completeness of the User's Manual and Library Model Document, and the effectiveness of documenting the update process.

The practicality of this metric depends on user cooperation in completing and forwarding the evaluation form. User information will be considered by the CARDS team when modifying the User's Manual, the Library Model Document and the README file. To what level of experience and knowledge is the User Manual written? Are specific items easily found by the experienced user? Do

users use the User Manual and do they provide feedback? What sections need clarifications? Do users read the README file? If not, why not? Do they find the information useful?

4. Operating Instructions

A. The User's evaluation is considered in modifying the contents of the "README" file. The users feedback will also identify the effectiveness of communication of changes within the CARDS teams.

The README file may contain information concerning the detection of a virus and corrective actions, changes in model relationships, training session updates, hardware, operational software, component software, system problems, corrective actions taken, etc. User feedback will aid in determining the content of, and the value of the information provided in, the README file.

Update metrics are related to other User Support metrics, and will directly affect Hotline Support metrics. If a user is not receiving update notices in a timely manner, this will generate numerous support calls inquiring about the updates/changes.

B. User Support personnel are responsible for collecting information about the quality of the documentation. The information is collected from user questionnaires, interviews, and hotline reports. The collection schedule is based on user feedback.

The following information is collected:

Did you read the User's Manual?

Is the manual understandable?

Do you use the manual to use the system and answer your questions?

How quickly can you locate the desired information?

Would training help you understand and use the manual?

The above information is gathered and evaluated. A Likert scale (1=poor, 5=good) or a binary scale is applied. The optimum level is 5 for the Likert scale and Yes for the binary questions. The critical level is 3 for the Likert scale and No for the binary questions.

User's Manual Metrics are related to other User Support metrics, and will directly affect Training metrics. If training is not performed to the needed level, the user will not be able to understand and use the manual.

5. Related Policies

9.1 METRICS DEFINITION CHANGE PROCESS

9.2 USER SUPPORT METRICS

9.3 SYSTEM METRICS - USER ACCOUNTS

9.4 SYSTEM METRICS - HARDWARE

9.5 SYSTEM METRICS - SOFTWARE

9.6 SYSTEM METRICS - TELECOMMUNICATIONS

9.7 INTEROPERABILITY METRICS

9.8 DOMAIN METRICS

9.9 COMPONENT EVALUATION METRICS

9.10 COMPONENT REUSE METRICS

9.11 COLLECTION OF METRICS - TRAINING

9.13 METRICS ANALYSIS AND PRESENTATION PROCESS

9.14 IMPLEMENTING METRICS ANALYSIS RESULTS PROCESS

6. Bibliography

None

9.13 METRICS ANALYSIS AND PRESENTATION PROCEDURE

Responsible Role: Library Administrator

Supporting Role(s): System Administrator, Component Engineer

1. Frequency

Each CCB and continuously on-line.

2. Preconditions

Metrics have been collected.

3. Goal

The goal is to provide interested parties with the information needed to understand the library process and needed process and product improvements.

4. Operating Instructions

5. This procedure applies only to regular, scheduled presentations to the CCB and on-line of metric data and analysis.

A. Briefings.

The procedure is to first set an end-of-month cutoff date for data. At least a week should be allowed after the cutoff date for data validation. Examine validated data for anomalies and trends. Analysis should account for and explain all items of interest. Another week should be allowed for analysis and charting. Data is then formed for presentation in the format specified for the CCB. NOTE: Since at least two weeks should be allowed for analysis and charting, any presentation in the first half of a month requires a cutoff date at the end of the second month back.

B. Charts Outline.

- Cover: Library Metrics, Briefer Name, Date
- Overview: Time frame, Goal, Question (User, System, Domain, Component)
- CARDS User Accounts: Air Force, Army, Navy, NSA, Industry, and Academia
- Hotline Requests: Information, Account
- CARDS Product Requests: documents
- Connect Time of CARDS Accounts: Cards Staff and Users, Number of Accounts/Minutes
- Remote Connections: Number of FTP, Telnet and total.
- Disk Usage: Library Software, Users, Model & Components, Applications, System, and Staff.
- Library Model Configuration: Name, Version Date, Concepts, Relation ships, and Lines.
- Component Evaluation: Defining/Refining Domain Criteria, Identified, Screened, Evaluated and Passed LCB.

C. CCB

After metrics information has been compiled and analyzed, the Library Administrator presents a summary at regular CCB meetings. Trends and areas that need improvement are pointed out as well as areas of growth. Projections are made concerning the growing user base of the library. Bottlenecks in user

support processes are identified and improvements are suggested. Any serious problems are submitted as action items subject to the CCBs resolution.

D. On-Line Presentation

To be determined

Charts from raw data will be built as software tools are acquired.

E. Metrics Presentation Matrix

Presentation of collected metric data and analysis must be audience specific. The possible audiences are Configuration Control Board, System Administrator, Library Administrator, Staff, Users, Management, Government, Program Manager, and other CARDS personnel.

Metric analysis with the indicated analysis interval will be presented as shown below:

METRIC	PMR	CCB	SYSADM	LIBADM	STAFF	USERS	MGMT	GOVT	PM	OTHER	ANYONE
USER SUPPORT	C	C	A	A	C	D	B	C	C	C	-
USER ACCOUNT	C	C	A	A	C	C	C	C	C	C	-
SYSTEM HARDWARE	C	C	A	A	C	C	C	C	C	C	C
SYSTEM SOFTWARE	C	C	A	A	C	C	C	C	C	C	C
SYSTEM TELECOMM.	C	C	A	A	C	C	C	C	C	C	-
INTEROPERABILITY	C	-	A	A	-	-	-	C	D	-	-
DOMAIN	C	C	B	A	C	C	C	C	C	C	-
COMPONENT EVALUATION	C	C	B	A	C	C	C	C	C	C	C
COMPONENT REUSE	C	C	B	A	C	C	C	C	C	C	C
TRAINING	D	D	D	D	D	D	D	D	D	-	-
LIBRARY DOCUMENTATION	D	D	D	D	D	D	D	D	D	-	-

ANALYSIS INTERVAL

A- DAILY B- WEEKLY C- MONTHLY D- ON-DEMAND

NOTE: Presentation intervals and metrics consumers have not been formally reviewed and approved. This draft version of the table is included in order to facilitate a discussion of presentation intervals.

Figure 9-1 Metrics Presentation Matrix

6. Related Policies

9.1 METRICS DEFINITION CHANGE PROCESS

9.2 USER SUPPORT METRICS

9.3 SYSTEM METRICS - USER ACCOUNTS

9.4 SYSTEM METRICS - HARDWARE

9.5 SYSTEM METRICS - SOFTWARE

9.6 SYSTEM METRICS - TELECOMMUNICATIONS

9.7 INTEROPERABILITY METRICS

9.8 DOMAIN METRICS

9.9 COMPONENT EVALUATION METRICS

9.10 COMPONENT REUSE METRICS

9.11 COLLECTION OF METRICS - TRAINING

9.12 LIBRARY DOCUMENTATION METRICS

9.14 IMPLEMENTING METRICS ANALYSIS RESULTS

7. Bibliography

None

9.14 IMPLEMENTING METRICS ANALYSIS RESULTS PROCESS

Responsible Role: Library Operations Project Lead

Supporting Role(s): Library Administrator, System Administrator

1. Frequency

Each release cycle.

2. Preconditions

Metrics have been collected and analyzed. The LCB and CCB have approved and prioritized proposed changes to the Library processes.

3. Goal

The goal of this process is to take action on the recommendations from the metrics analysis. What process improvements are suggested? Where? Which process steps need to be further refined for metrics definition and collection? Which

processes are stable? What processes should be added to data collection? What process changes are necessary and what is the expected cost/benefit of these changes? What improvements are indicated in the Library's products? Where should process steps be changed to affect product improvements?

4. Operating Instructions

   A. The Library Operations Project Lead evaluates processes recommended for change for impact on staff and schedule.

   B. The Project Lead works with the library staff to modify the processes based on the metrics findings.

   C. Related documentation is updated and useful metrics are added to the LOPP at its regularly scheduled updates.

5. Related Policies

   9.1 METRICS DEFINITION CHANGE PROCESS

   9.2 USER SUPPORT METRICS

   9.3 SYSTEM METRICS — USER ACCOUNTS

   9.4 SYSTEM METRICS — HARDWARE

   9.5 SYSTEM METRICS — SOFTWARE

   9.6 SYSTEM METRICS — TELECOMMUNICATION

   9.7 INTEROPERABILITY METRICS

   9.8 DOMAIN METRICS

   9.9 COMPONENT EVALUATION METRICS

   9.10 COMPONENT REUSE METRICS

   9.11 COLLECTION OF METRICS — TRAINING

   9.12 LIBRARY DOCUMENTATION METRICS

   9.13 METRICS ANALYSIS AND PRESENTATION PROCESS

6. Bibliography

   None

APPENDIX A - Forms

The Forms List chapter shows those forms previously discussed in the Library Operations Policies and Procedures Manual. The forms are blank so that users can copy and apply them, as needed, to their respective Library environments.

CENTRAL ARCHIVE FOR REUSABLE DEFENSE SOFTWARE (CARDS)

Hotline Correspondence Log 1.0

Date	Incoming Outgoing Phone E-mail	Number Called	Name	Account Name	Subject	Referred To	HLR Number	Operator

Figure A-1 Hotline Correspondence Log 1.0

CARDS
Central Archive for Reusable Defense Software
CARDS Library Account Registration Form (CLARF)
Version 3.1
Effective May 17, 1993

INSTRUCTIONS

1) Complete all items on this form. All of the following requested information MUST BE completed before an account will be activated.
2) Please print or type.
3) Sign and date form.
4) Obtain authorized signature and date.
5) Return the completed form by mailing to:

CARDS Command Center Library
ATTN: CARDS User Support - CLARF
1401 Country Club Road, Suite 201
Fairmont, WV 26554

ORGANIZATIONAL INFORMATION

Name:_____

Title/Rank:_____

Company Name/Service:_____

Office Symbol/Code:_____

Street Address:_____

City/Base/Military Station:_____

State:_____ Zip Code:_____

Country:_____

Daytime Phone Number (Non-DSN Number):_____ Ext:_____

Fax Number:_____

E-Mail Address:_____

GOVERNMENT CONTRACT INFORMATION

Are You a United States Citizen? ( )Yes ( )No

Are you a Government Employee? ( )Yes ( )No

Are You a Government Contractor/Subcontractor? ( )Yes ( )No

Government Program/Project:_____
(If you are working on more than one project/program, please provide the most appropriate.)

Government Contract Number:_____

Government Contract Expiration Date:_____

Purpose for requesting an account:_____

_____

_____

_____

Where did you hear about CARDS? (example: Articles, conferences, etc.)

_____

_____

UNIQUE IDENTIFICATION INFORMATION

Enter any four keyboard characters. This will NOT be your password; but you will need this for security and validation purposes.

____-____-____-____

COMPUTER/TERMINAL INFORMATION

Please identify someone in your organization that we may contact for information about your system.

Systems Administrator Name:_____

Systems Administrator Phone:_____

Please note the IP addresses and corresponding names for all machines from which you will access the CARDS library. (The IP number is an address, assigned by DDN Network Information Center, for uniquely identifying machines on a world wide network.)

IP#:	IP#:
IP#:	IP#:
IP#:	IP#:
IP#:	IP#:
IP#:	IP#:

COMPANY/AGENCY INFORMATION

1. What is your primary business activity?

   ( )Air Force ( )Marine Corps
   ( )Army ( )Navy
   ( )Coast Guard ( )DoD
   ( )Other (NSA, NASA, etc.) Please specify:_____

2. What is your primary job function?

   ( )Data Processing ( )Programming
   ( )Executive SES ( )Program Manager
   ( )Maintainence ( )Research/Development
   ( )Management ( )Software Engineering
   ( )Operations ( )Systems Integration/Design
   ( )Planning ( )Test/Evaluation
   ( )Procurement ( )Other, please specify:_____

3. Are you a member of any Reuse special interest groups? (example: SIGAda, RIG)

   ( )No ( )Yes, please list:_____

4. Have you ever used a software reuse library?

   ( ) No ( ) Yes, please list:_____

5. Have you received a copy of the CARDS Brochure? ( ) No ( ) Yes

ORGANIZATIONAL AUTHORIZATION

Please include an authorized signature from one of the following:
Program Manager, Task Coordinator, Project Lead, etc.

Authorized by:_____ Date:_____
Please Print Name & Title/Rank

Address: _____

_____

_____

Phone: ( )_____

_____

Signature

ACCOUNT HOLDER AGREEMENT

I have read the CARDS Library Account Holder Rights and Responsibility Statement and do hereby understand and agree to the terms, conditions and restrictions stated therein. The User and CARDS agree that the CARDS Library Account Holder Rights and Responsibility Statement shall be governed by the Laws of the United States of America.

Applicant's Name:_____ Date:_____
Please Print

_____
Signature

Figure A-2 CARDS Library Account Registration Form (CLARF)

CENTRAL ARCHIVE FOR REUSABLE DEFENSE SOFTWARE (CARDS)

Authorization Sheet 1.0

For Official Use By User Support Team
Printed Name: _____ Date: _____
Authorized Signature: _____
Approved ( ) Disapproved ( ) Why: Staff ( ) Staff Affiliate ( ) User ( )
Add to: CARDS_TEAM ( ) CARDS_MGT ( ) USERS ( ) OTHER ( )
Activated By: _____ Date: _____
Tested By: _____ Date: _____
Notified By: _____ Date: _____
For Official Use By System Administrator
Unix Account Name: _____ Date of Activation: _____ Unix UID: _____ Date of Deactivation: _____ Password: _____
AFS Account Name: _____ Date of Activation: _____ AFS UID: _____ Date of Deactivation: _____ Password: _____

Figure A-3 Authorization Sheet 1.0

CARDS ACCOUNT ACTIVATION LOG

For the week of _____ to _____

Name	Chk info	Date rec'd	Authorize sent	Authorize rec'd	Activate sent	Activate rec'd	TCP Wrap sent	TCP Wrap rec'd	Interoperation sent	Interoperation conf	Aliases	Password disabled	Mailbox	Username

Figure A-4 CARDS Account Activation Log 1.0

CARDS ACCOUNT DEACTIVATION LOG

For the week of _____ to _____

Name	Company	I/G/A	Date of deactivation sent/conf		Interop sent sent/conf		Removed from alias

Figure A-5 CARDS Account Deactivation Log 1.0

Requests for the week of to

User Name and Address	Date	Phone E-Mail	URF	Info	Miscellaneous	Date to PM	Date PM Rec'd	Date mailed	Rep'd

Figure A-6 CARDS Request Log

Hotline Reports (open/resolved issues)Log

For the week of _____ to _____

Date	Hotline Report #	User Name	Date Ack Sent	Issue	Forwarded to	Date forwarded	Date Resolved	Date Res Sent	On-line	Reported

Figure A-7 Hotline Reports (open/resolved issues) Log

S W O's (open/resolved issues) Log

For the week of _____ to _____

Date	SWO #	Staff Name	Date Ack Sent	Issue	Forward to	Date forward	Date resolved	Date Res sent	On-line	Rep'd

Figure A-8 SWO's (open/resolved issues) Log

HOTLINE REPORT 1.0

HLR#: _____

User Information

Name: Verified ( )
Rank/Title:
Company Name/Government Agency:
Physical Address:

E-mail Address:
Phone:
Fax:

Best Time to Contact:
Alternate Point of Contact:
Account Name:

Type of Hardware:
Type of Software:
Type of LAN:

Issue Reported

Operator Name:
Date and Time Reported:
Time Acknowledgement Notice Sent:

Nature of Problem:

Task Attempted:

Steps Taken:

Results:

Steps Taken to Correct Problem:

Results:

HOTLINE REPORT 1.0

Date: _____ HLR#: _____

	NAME	FMT/CMT/UST	DATE
Submitted By:			
Forwarded To:			
Resolved By:			

Estimated Time of Problem Resolution:

Detailed, Step-by-Step Solution:

Time Required for Problem Resoluiton:

Date Resolved Letter Sent:

Figure A-9 Hotline Report 1.0

CENTRAL ARCHIVE FOR REUSABLE DEFENSE SOFTWARE (CARDS)

STAFF WORK ORDER 1.0

Staff Information

Name:

Company Name:

Location:

Order

Date and Time:

Nature of Work:

CENTRAL ARCHIVE FOR REUSABLE DEFENSE SOFTWARE (CARDS)

STAFF WORK ORDER 1.0

Staff Information

Name:

Company Name:

Location:

Order

Date and Time:

Nature of Work:

Figure A-10 Staff Work Order 1.0

APPENDIX B - GLOSSARY

Account Activation Log	An administrative form used to track each step of the account activation process.
Account Deactivation Log	An administrative form used to track each step of the account deactivation process.
AFS	A distributed, wide-area network file system.
application domain	The knowledge and concepts which pertain to a particular computer application.
authorized user	A library user that has completed the user registration process, has been approved by the CARDS program management, and has been as signed an access authorization number.
browse	Surveying the reusable component descriptions in a library to determine whether the component is applicable to the current application.
caller	An individual who calls the library hotline.
command center	A facility from which a commander and his/her representatives direct operations and control forces. It is organized to gather, process, analyze, display and disseminate planning and operational data and to perform other related tasks.
commercial off-the-shelf (COTS)	Commercially available software.
common criteria	Attributes used to evaluate a component regardless of the domain. See component certification.
component	A set of reusable resources that are related by virtue of being the inputs to various stages of the software life cycle, including requirements, design, code, test cases, documentation, etc. Components are the fundamental elements in a reusable software library.
component certification	The process of determining that a component being considered for inclusion in the library meets the requirements of the library and passes all testing procedures. Evaluation takes place against a common set of criteria (reusability, portability, etc.).
component management	The process of component acquisition, evaluation, certification, testing, and maintenance.

component qualification	The process of determining that a potential component is appropriate to the library and meets all quality requirements. Evaluation takes places against domain criteria.
Configuration Control Board (CCB)	The authority that is responsible for configuration management.
configuration management	A discipline for managing change.
countermeasure	Procedure to alleviate a threat identified during the Security Analysis.
developer	1) One who aids in the development of the command center library. 2) One who accesses the CARDS library with the intent of retrieving components for use in developing systems for domain-specific applications.
domain	An area of activity or knowledge containing applications which share a set of common capabilities and data.
domain analysis	The process of identifying, collecting, organizing, analyzing, and representing the relevant information in a domain based on the study of existing systems and their development histories, knowledge captured from domain experts, underlying theory, and emerging technology within the domain.
domain architecture	High-level paradigms and constraints characterizing the commonality and variances of the interactions and relationships between applications within a domain.
domain criteria	Specifications a component must adhere to in order to obtain acceptability in the domain. See component qualification.
domain engineering	An encompassing process which includes domain analysis and the subsequent construction of components, methods, tools, and supporting documentation that address the problems of system/subsystem development through the application of the knowledge in the domain model and soft ware architecture.
domain expert	An individual who is knowledgeable in a domain.
domain-level integration	The process of using and evolving domain and application components in the creation of requirements, architectures and implementations (domain and application).

domain model	A definition of the functions, objects, data, and relationships in a domain, consisting of a concise representation of the commonalities and differences of the problems of the domain and their solutions.
domain modeling	The process of encoding knowledge about a domain into a formalism.
domain-specific library	A library whose components are bound by a specific domain.
domain-specific reuse	Reusing components in a specific domain (through the use of a domain- specific library) to build an instance of an application in that domain.
domain-specific software architecture	An architecture (interactions and relationships between objects) used to develop software applications based on a specific domain.
franchise	An instance of a library-centered domain-specific infrastructure built utilizing the CARDS Concept of Operations/Franchise Plan.
franchisee	An organization (government, contractor, commercial, educational) that is committed to developing a domain-specific reuse capability that includes: reciprocal obligations and a cooperative partnership with a franchise. has a business agreement with a franchise that enumerates the range and level of services, training and education and technology transfer to be provided by a franchise and obtained from the franchisee. shares a model-based, library-assisted technical vision with the organization to whom a franchise is granted.
generic architecture	High-level paradigms and constraints that characterize the commonality and variances of the interactions and relationships between the various components in a system.
generic command center architecture	The fundamental generic architecture that underlies command center applications.
government off-the-shelf (GOTS)	Software developed for and owned by the government.
graphical browser	A graphical presentation of the domain model and interrelations between components. Through the graphical

	browser, components may be browsed, viewed, and extracted. It also provides an inferencing mechanism to aid in prototyping and selecting the correct components.
Hotline Report	An administrative report used to track a Hotline Request throughout the resolution process.
Hotline Report Log	An administrative form used to log all current open issues and previously resolved Hotline Reports.
interoperability	The ability of two or more systems to exchange information and to mutually use the information that has been exchanged.
knowledge blueprint	A flexible plan to transition knowledge to the community.
knowledge representation	Codification of domain knowledge.
library	A collection of components that are cataloged according to a common classification scheme and a set of applications that provide a mechanism to browse and retrieve components.
library account holder	A user or staff member who is authorized to access the library. There are currently five account types which an account holder may be as signed to a library account holder: Staff Developer Account - holders of this account type have a typical Unix account and an AFS account with RLF development directory privileges. Staff Account - holders of this account type have a typical Unix and an AFS account with restrictions in RLF development directories. Staff Affiliate Account - holders of this account type have a typical Unix account and an AFS account with restrictions in RLF development directories and the living documents directory. Users with Sun4 and AFS - holders of this account type will have an AFS account only, with restrictions in RLF development directories and in the living documents directory. Users without AFS or without Sun4 - holders of this account type have a restricted Unix account and an AFS account with restrictions in RLF development directories and in the living documents directory.
library applications	Services provided to the library user.

library-centered domain-specific reuse	Reusing components in a specific domain to build an instance of an application in that domain utilizing a domain specific reuse library.
Library Control Board (LCB)	The deliberative body which controls the decision-making process for making recommendations about library components (e.g., which components to acquire, reject, or modify). The LCB also has approval authority for determining when to release new versions of a library to the Configuration Control Board for customer release. The LCB is concerned with the technical issues related to library construction.
library model	A model that represents the domain components and the relationships be tween them.
library system	A collection of one or more domain-specific libraries that can be accessed using the same operational hardware and software.
life cycle	All the activities (e.g., design, code, test) a component is subjected to from its inception until it is no longer useful. A life cycle may be modeled in terms of phases, which are often characterizations of activities by their purpose or function such as design, code, or test.
life-cycle artifact	A product of the software engineering process (i.e., a component).
memorandum of understanding (mou)	An agreement stating terms of cooperation between two entities.
metric	Quantitative and qualitative analysis values calculated and collected according to a precise definition and used to establish comparative aspects of development progress, quality assessment, or choice of options.
RLF	Reuse Library Framework. Provides a framework for building domain-specific libraries.
repository	The mechanism for defining, storing, and managing all information, concerning an enterprise and its software systems - logical data and process models, physical definitions and code, and organization models and business rules.
Request Log	An administrative form used to track the types of information each user requests. Examples of such informa-

	tion includes: the Information Packet, the User Recruit Packet, the Component Packet, and documentation.
reusable component	A component (including requirements, designs, code, test data, specifications, documentation, expertise, etc.) designed and implemented for the specific purpose of being reused.
reuse	The application of existing solutions to the problems of system development. Reuse involves transfer of expertise encoded in software-related work products. The simplest form of reuse from software work products is the use of subroutine/subprogram libraries for string manipulations or mathematical calculations.
reuse library	A library specifically designed, built, and maintained to house reusable components.
reuser	One who implements a system through the reuse process.
role	Title denoting staff member(s) responsible for performing actions as specified.
rule base	A collection of rules about the elements of a domain. A rule describes when and how the facts about the model may change.
Rule Base Definition Language (RBDL)	An application specific language (ASL) used to define AdaTAU inference bases.
security testing	A type of testing in which testers determine whether the security features of a system are implemented as designed. Security testing may include hands-on functional testing, penetration testing, and formal verification.
semantic network	A graphical knowledge representation method composed of nodes linked to each other.
Semantic Network Definition Language (SNDL)	An application specific language (ASL) used to define AdaKNET semantic network models.
staff	Personnel who physically work for the specified library.
staff work order	Request from the staff to suggest enhancements to the operational library system. Staff work orders are typically forwarded to the CCB, unless immediate resolution is possible.

SWOs Log	An administrative form which logs all current open issues and previously resolved Staff Work Orders.
system architecture	A model that represents the interrelationship between system elements and sets a foundation for later requirements analysis and design steps.
system composition	The automatic configuration of a prototype system based on hardware and software requirements.
system engineering	A process encompassing requirements gathering at the system level with a small amount of top-level design and analysis.
user	An individual assigned an access authorization number and authorized to access the library to develop systems for domain-specific applications.
user account	The physical account established for each user containing pertinent information relative to that user.
user account log	A record of information pertaining to the stages of the enrollment and de activation process for each user.
user registration	The process of enrolling a potential library user.
user registration form (URF)	The initial form to be completed by a potential user in order to become an authorized library user. It is included in Volume Two, Operational Instructions.
user support	All functions related to the technical and administrative support of the end user.
work order	Request for changes to be made to the operational system. The work orders are typically given from the CCB to the System Administrator.

APPENDIX C - BIBLIOGRAPHY

[AFS92] AFS System Administration Guide, July 1992.

[BASILI92] Basili, Victor R, "Software Modeling and Measurement: The Goal/Question/Metric Paradigm", University of Maryland, 1992

[CARDS93a] Technical Concept Document, CARDS, Informal Technical Report, STARS-AC-04107A/001/01, February 26, 1993.

[CARDS93b] Franchise Plan, CARDS, Informal Technical Report, STARS- AC-04116-000-00, March 30, 1993.

[CARDS93c] ASSET/CARDS/DSRS Library Interoperation, Informal Technical Report/Informal delivery item, July 15, 1993.

[CARDS93d] Library Development Handbook, CARDS, Informal Technical Report, STARS-VC-B005/001/00, October 29, 1993.

[CARDS94a] Library Operations Policies and Procedures Volume I, CARDS, Informal Technical Report, STARS-VC-B004/002/00, February 28, 1994.

[CARDS94b] Library Operations Policies and Procedures Volume II, CARDS, Informal Technical Report, STARS-VC-B004/001/01, September 30, 1993.

[CARDS94c] User Rights & Responsibilities Statement 2.0, Library Operations Policies and Procedures Volume I, CARDS, Informal Technical Report, STARS-VC-B004/002/00, February 28, 1994.

[MOU93a] Central Archive for Reusable Defense Software and Asset Source for Software Engineering Technology Memorandum of Understanding for Asset Exchange, April 29, 1993

[MOU93b] Central Archive for Reusable Defense Software and Defense Software Repository System Memorandum of Understanding for Asset Exchange, April 29, 1993

[SYBASE92] System Administration Guide for Sybase SQL Server, Release 4.9.1, 15 October 1992..

[UNIX91] Unix System Administration 4.1.2, SA 270, Student Guide, April 1991.